Reglamento General de Gestión en Tecnologías de Información

CONASSIF 1318 y 1319 del 13 y 20 de Marzo del 2017
Publicado en el Alcance a la Gaceta No.80 del 17 de Abril del 2017

SUGEF Superintendencia General de Entidades Financieras
SUPEN Superintendencia de Pensiones
SUGESE Superintendencia General de Seguros República de Costa Rica
SUGEVAL Superintendencia General de Valores

Agenda

1. Consideraciones generales
   a) Estructura de la norma
   b) Justificación desde la perspectiva de gestión y control de TI
   c) Supervisión Basada en Riesgos
   d) Estándares y mejores prácticas disponibles como marco de referencia
   e) Estrategia de supervisión
   f) Auditoría externa y registro de auditores

2. Reglamento y lineamientos de TI
   a) Alcance
   b) Unidad de TI
   c) Gobierno de TI
   d) Gestión de TI
   e) Perfil tecnológico
   f) Tipo de gestión
   g) Proceso del reglamento
   h) Proceso de auditoría
   i) Bases de datos
   j) Plazos

Consideraciones generales

Estructura

a) Estructura de la Norma

Estructura de la Norma

Capítulo I: Disposiciones Generales

Capítulo II: Organización de las TI

Capítulo III: De la Supervisión y la Auditoría Externa de TI

Estructura de la Norma

Capítulo I: Disposiciones Generales

- Artículo 1: Objeto
- Artículo 2: Alcance
- Artículo 3: Definiciones y abreviaturas
- ***Artículo 4: Lineamientos Generales***
- Artículo 5: Coordinación entre superintendencias

SUGEF SUPEN SUGESE SUGEVAL

Estructura de la Norma

Capítulo II: Organización de la TI

- Artículo 6: Unidad de TI
- Artículo 7: Gobierno de TI
- Artículo 8: Gestión de TI

Estructura de la Norma

Capítulo III: De la Supervisión y la Auditoría Externa de TI

- ***Sección I: Perfil tecnológico y Tipo de Gestión de TI***
  - ***Artículo 9: Perfil tecnológico***
  - ***Artículo 10: Tipo de gestión de TI***

Estructura de la Norma

Capítulo III: De la Supervisión y la Auditoría Externa de TI

- ***Sección II: Auditoría Externa de TI***
  - ***Artículo 11: Auditoría de las Tecnologías de Información***
  - ***Artículo 12: Alcance y plazo de la auditoría***
  - ***Artículo 13: Productos entregables***
  - ***Artículo 14: Presentación de resultados de la auditoría externa de TI***

Estructura de la Norma

Capítulo III: De la Supervisión y la Auditoría Externa de TI

- ***Sección III: Reporte supervisor y plan de acción***
  - Artículo 15: Reporte de Supervisión
  - ***Artículo 16: Plan de acción***

SUGEF SUPEN SUGESE SUGEVAL

Estructura de la Norma

Capítulo III: De la Supervisión y la Auditoría Externa de TI

- ***Sección IV: Prórrogas y Calificación de riesgos de TI***
  - Artículo 17: Prórrogas
  - Artículo 18: Calificación de riesgos de TI

Estructura de la Norma

Capítulo III: De la Supervisión y la Auditoría Externa de TI

- ***Sección V: Bases de datos***
  - Artículo 19: Bases de datos

Justificación

b) Desde la perspectiva de gestión y control de TI

Justificación

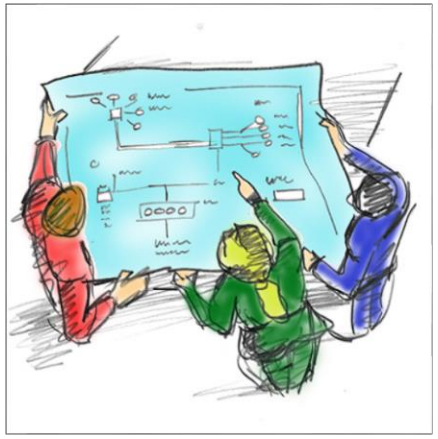
- **Gestión de TI**
  - Entidades supervisadas son responsables de establecer la gestión de TI, considerando:
    - Los procesos descritos en los Lineamientos Generales
    - Los riesgos de TI (gestión integral de riesgos)

Justificación

- **Gobierno de TI**
  - Disposiciones en las que resaltan la necesidad de mejorar los sistemas de **Gobierno Corporativo** y en consecuencia, la forma de **gobernar la TI**.

Funciones del órgano directivo y comité de TI: El Reglamento de Gobierno Corporativo

Justificación



TI es visto como un proceso más del negocio

TI como un proveedor de servicios para mantener la **plataforma** y los **sistemas** que **apoyan** el resto de *los procesos del negocio*.

SUGEF SUPEN SUGESE SUGEVAL

Justificación

Necesidad de control y gestión de TI

- **Inadecuada gestión** del **riesgo operacional** en el área de la TI.
- Repercusión **negativamente** en la **continuidad** de las **operaciones**.
- Impactando en el **patrimonio** de las **entidades** y concomitantemente, **afectando** a los **clientes** de las entidades.

Justificación

Necesidad de control y gestión de TI

- Determinar los **requerimientos mínimos** de *gestión* y *control*.
- Garantizar la seguridad, y auditabilidad de la información y de los servicios ofrecidos.
- La exposición de los servicios a consulta o transaccionales a través de Internet.

Supervisión Basada en Riesgos

c) SBR

Supervisión basada en riesgos

- Migración de un modelo basado en reglas hacia un **enfoque** donde la entidad supervisada es **responsable** de una **gestión integral** de los **riesgos del negocio**.

Supervisión basada en riesgos

- La **entidad** determinará, dentro de esa **gestión de riesgos**, el **marco de gestión** de TI.
- Identificar y establecer las **medidas de mitigación** para los riesgos de TI.

Supervisión basada en riesgos

- La regulación se enfoca a **requerir un marco** de gestión de TI **con aquellas características prudenciales suficientes** para el supervisor.

- Enfoque en el cual la entidad es responsable de una gestión integral de los riesgos del negocio, incluido el riesgo tecnológico

Supervisión basada en riesgos

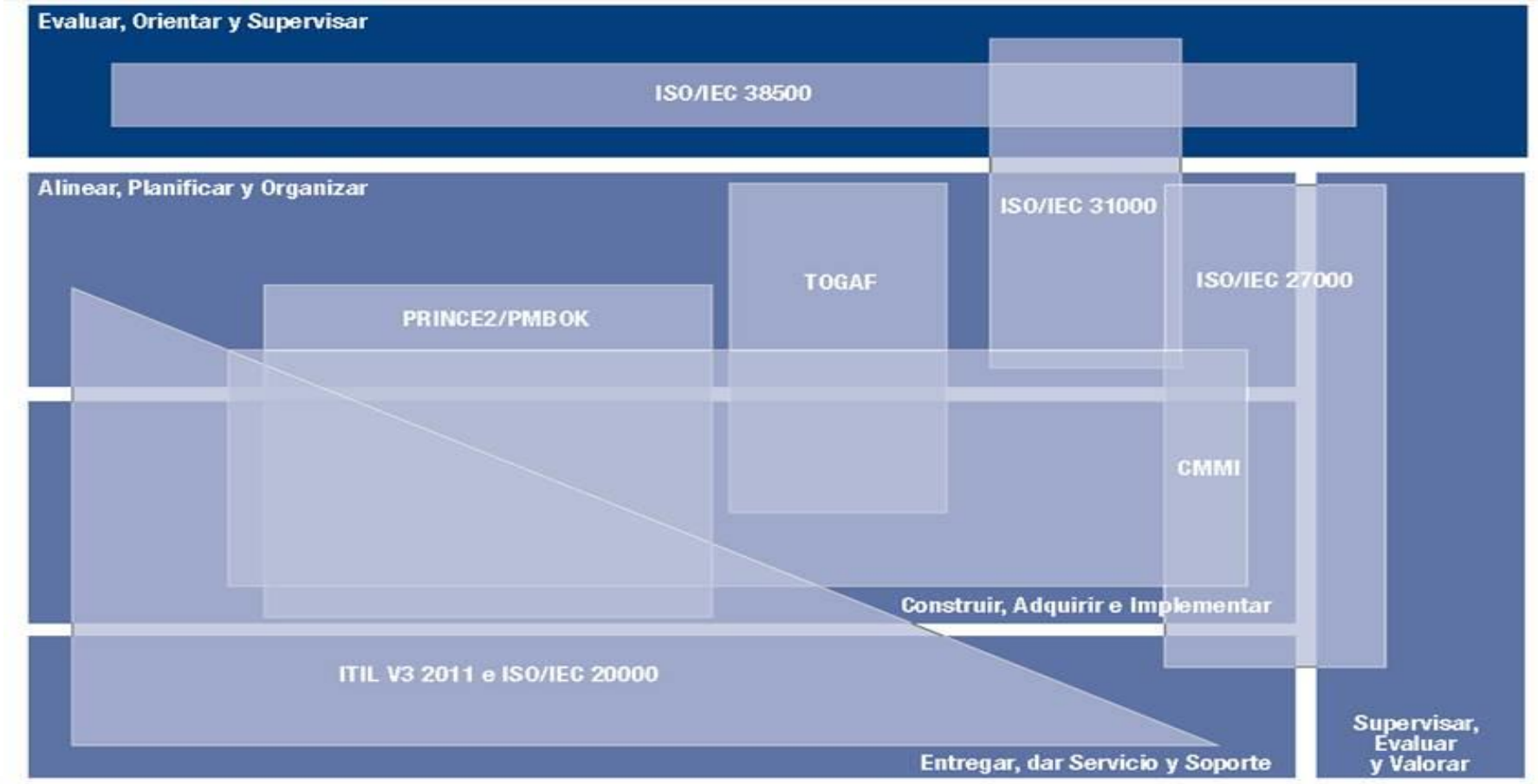
- El reglamento es parte de una estructura normativa **transversal** al sistema financiero.
- Nutre el proceso de supervisión a partir del aporte de especialistas externos.

Estándares

d) Estándares y mejores prácticas disponibles como marco de referencia

Estándares y mejores prácticas

- La industria y los profesionales en TI, han venido desde hace varias décadas desarrollando estándares y marcos que permitan gestionar y controlar la TI.



Estrategia

e) Estrategia de supervisión

Estrategia de supervisión

- Un solo cuerpo normativo.
- Requerimientos mínimos de gestión.
- Estandarización de procesos.
- Generación de economías de escala.
- Creación de una cultura proclive a la mejora de la gobernabilidad de la TI.

Resolvió:

I. Aprobar el *Reglamento General de Gestión de la Tecnología de Información* conformidad con el siguiente texto:

REGLAMENTO GENERAL DE GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto

Este Reglamento establece los requerimientos mínimos para la gestión de la tecnología de información que deben acatar las entidades supervisadas y reguladas del sistema financiero costarricense.

Artículo 2. Alcance

Las disposiciones establecidas en este Reglamento son de aplicación para:

a) Supervisados por SUGEF:
1. Bancos comerciales del Estado;
2. Bancos creados por ley especial;
3. Bancos privados;
4. Empresas financieras no bancarias;
5. Organizaciones cooperativas de ahorro y crédito;
6. Mutuales de ahorro y préstamo y
7. Caja de ahorro y préstamos de la ANDE;
8. Cualquier otro intermediario financiero sujeto a supervisión por SUGEF.

b) Supervisados por SUGEVAL:
1. Puestos de Bolsa y Sociedades Administradoras de Fondos de Inversión;
2. Bolsas de Valores;
3. Sociedades de compensación y liquidación;
4. Proveedores de Precio;
5. Entidades que brindan servicios de custodia;
6. Centrales de Valores;
7. Sistemas de Anotación Electrónica en Cuenta, y
8. Sociedades titularizadoras y fiduciarias.

Estrategia de supervisión

- **Grado** de **dependencia** de TI.
- La materialización de los riesgos.
- Proporcionalidad que rige los esquemas de supervisión basada en riesgo para SBR.

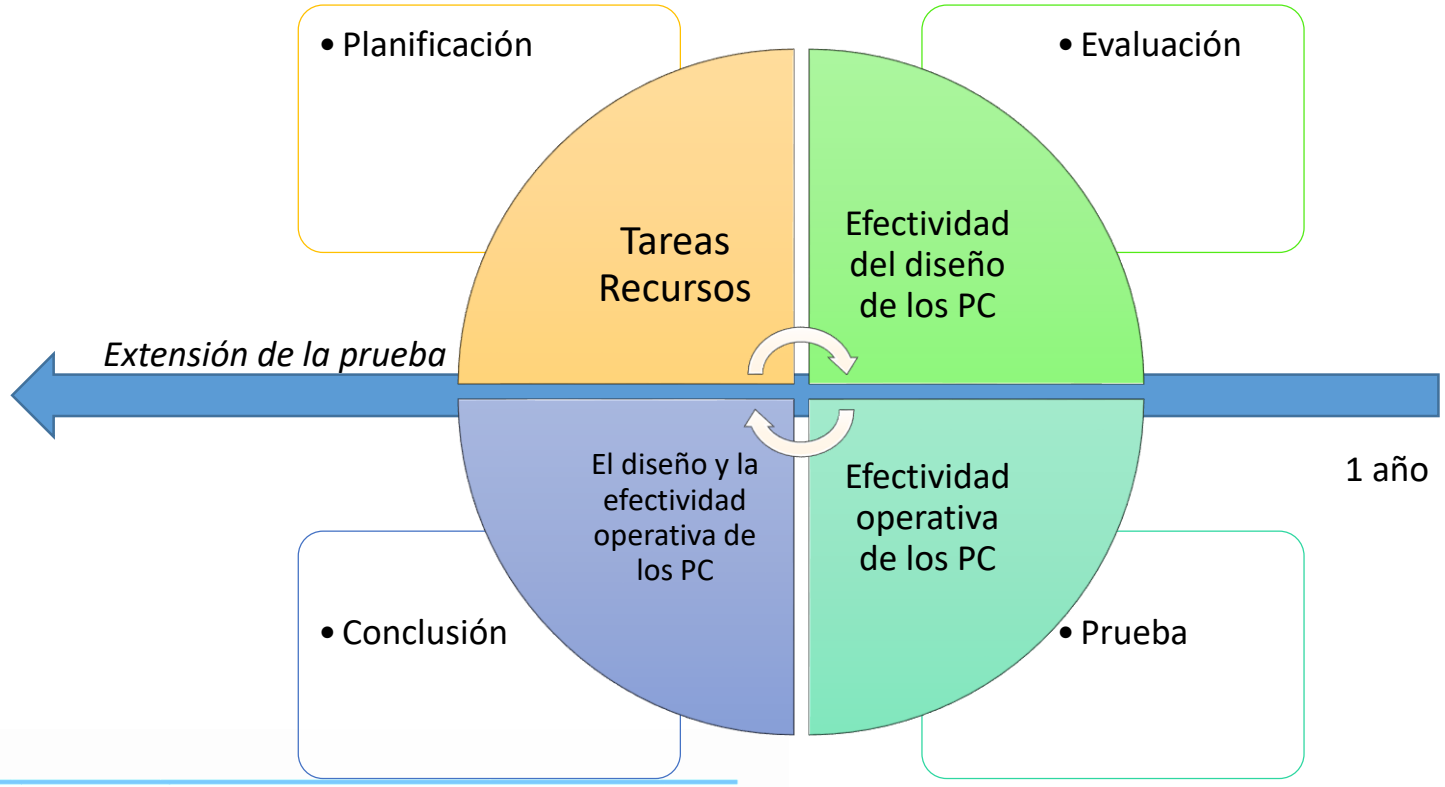
Auditoría y registro

f) Auditoría externa y registro de auditores

Auditoría externa y registro de auditores

Tipo de auditoría

- Auditoría directa que brinde un alto nivel de aseguramiento acerca de la efectividad de los procesos de control.



SUGEF SUPEN SUGESE SUGEVAL

PC: Procedimientos de Control

Auditoría externa y registro de auditores

Considera el criterio de terceros

- La **revisión** del marco de gestión de TI sea **ejecutada por auditores externos** con el fin de contribuir con la eficiencia en el proceso de supervisión.
- Insumo al proceso de SBR.

Auditoría externa y registro de auditores

Registro de auditores elegibles

- Se amplía el alcance de este registro para que incluya a los auditores externos de tecnologías de la información.
- Se establecen requerimientos de idoneidad para los auditores y firmas auditadas.

Reglamento y Lineamientos

Requerimientos mínimos para la gestión de la tecnología de información

Alcance

a) Alcance

Supervisados por SUGEF

- Bancos comerciales del Estado
- Bancos creados por ley especial
- Bancos privados
- Empresas financieras no bancarias
- Organizaciones cooperativas de ahorro y crédito
- Mutuales de ahorro y préstamo y
- Caja de ahorro y préstamos de la ANDE
- Cualquier otro intermediario financiero sujeto a supervisión por SUGEF

Supervisados por SUPEN

- Operadoras de Pensiones Complementarias
- Fondos complementarios creados por leyes especiales o convenciones colectivas
- Regímenes públicos sustitutos del Régimen de Invalidez, Vejez y Muerte de la Caja Costarricense de Seguro Social

Grupo o Conglomerado Financiero

- Banco
- Puesto de Bolsa
- Operadora de Pensiones Complementarias
- Aseguradoras

Supervisados por SUGEVAL

- Puestos de Bolsa y Sociedades Administradoras de Fondos de Inversión
- Bolsas de Valores
- Sociedades de compensación y liquidación
- Proveedores de Precio
- Entidades que brindan servicios de custodia
- Centrales de Valores
- Sistemas de Anotación Electrónica en Cuenta
- Sociedades titularizadoras y fiduciarias

Supervisados por SUGESE:

- Entidades Aseguradoras y sociedades Reaseguradoras
- Sucursales de entidades aseguradoras extranjeras

SUGEF SUPEN SUGESE SUGEVAL

Artículo 6: Unidad de TI

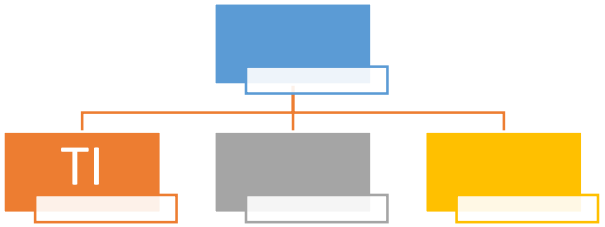
b) Unidad de TI

Artículo 6: Unidad de TI

- Es la estructura que provee los procesos y servicios de TI.

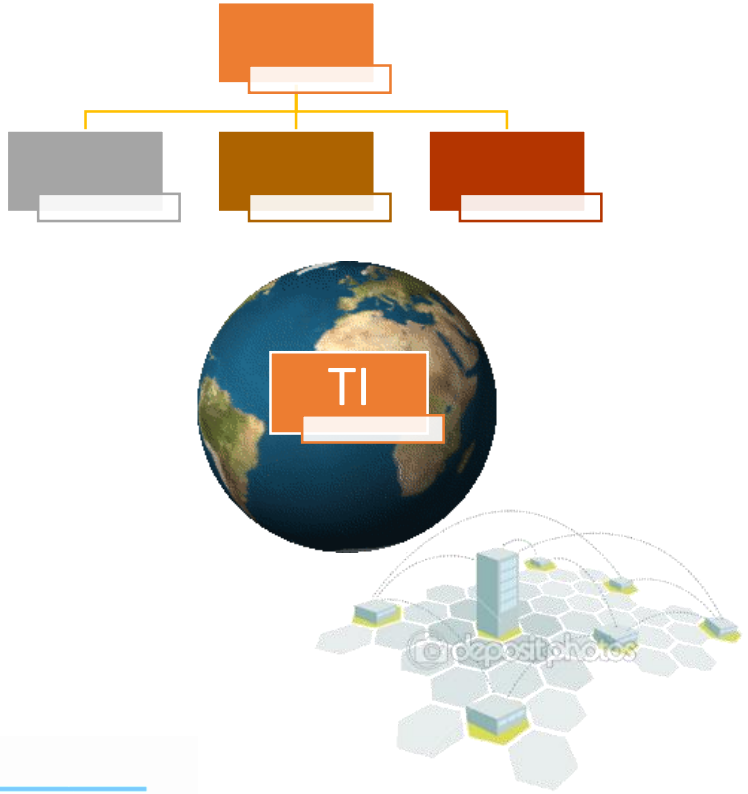
Ubicación de la Unidad de TI - Individual

Forma parte de la estructura organizativa



Proveedor externo domiciliado en Costa Rica

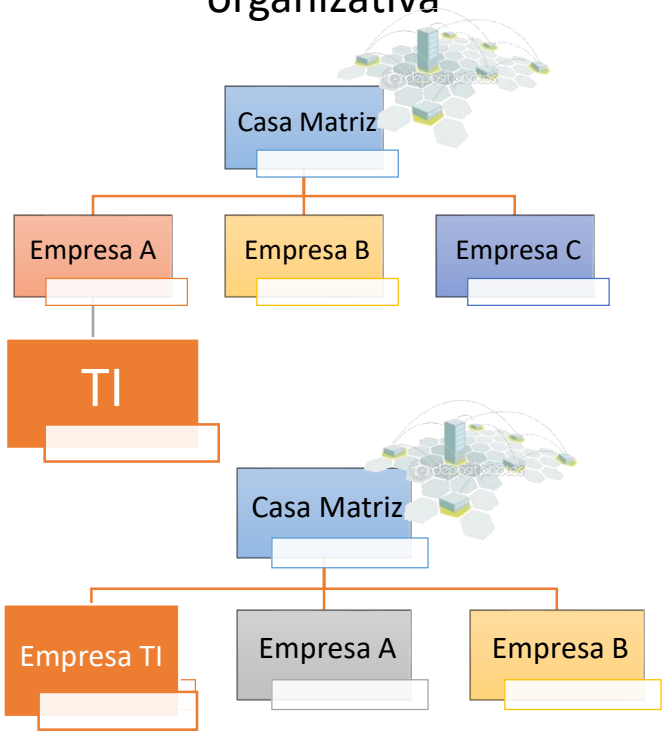
Proveedor externo domiciliado fuera de CR



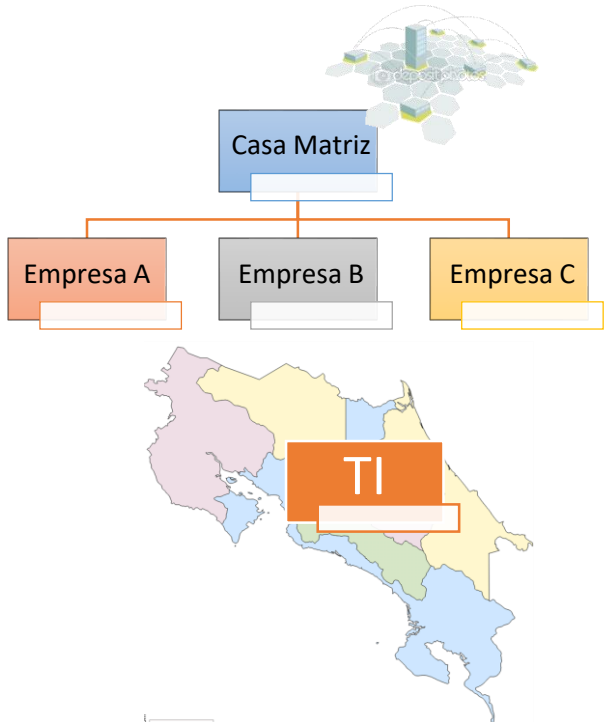
SUGEF SUPEN SUGESE SUGEVAL

Ubicación de la Unidad de TI - Corporativo

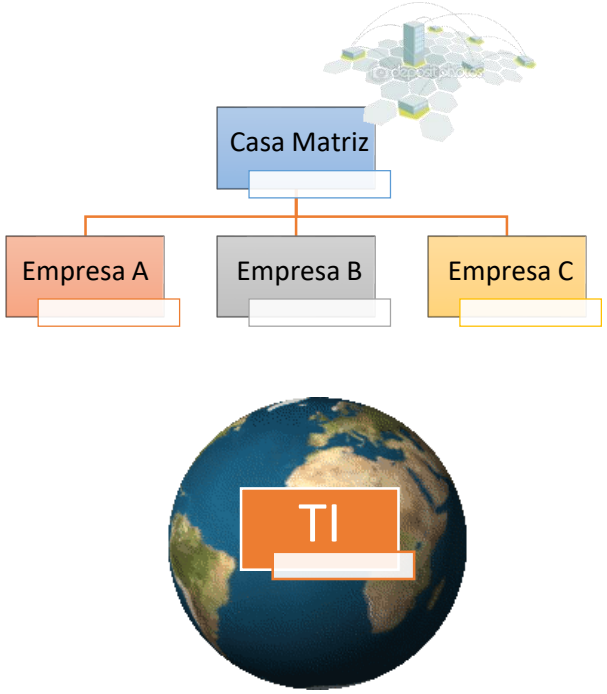
Forma parte de la estructura organizativa



Proveedor externo domiciliado en Costa Rica



Proveedor externo domiciliado fuera de CR



Artículo 7: Gobierno de TI

c) Gobierno de TI

Artículo 7: Gobierno de TI

- Las entidades deben establecer una estructura de gobierno de TI orientada a:
  - Generar **valor**
  - Conseguir **beneficios**
  - Acorde a los niveles de **riesgo** aceptables
  - Uso óptimo de los **recursos** de las tecnologías de la información.

- Las entidades supervisadas deben procurar que:
  - Las **necesidades de las partes interesadas** sean evaluadas respecto a las metas corporativas establecidas;
  - instituir una **dirección** del gobierno y de la gestión de TI priorizada;
  - asegurar que sea **monitoreado el rendimiento y el cumplimiento** respecto a la dirección y las metas acordadas.

Artículo 8: Gestión de TI

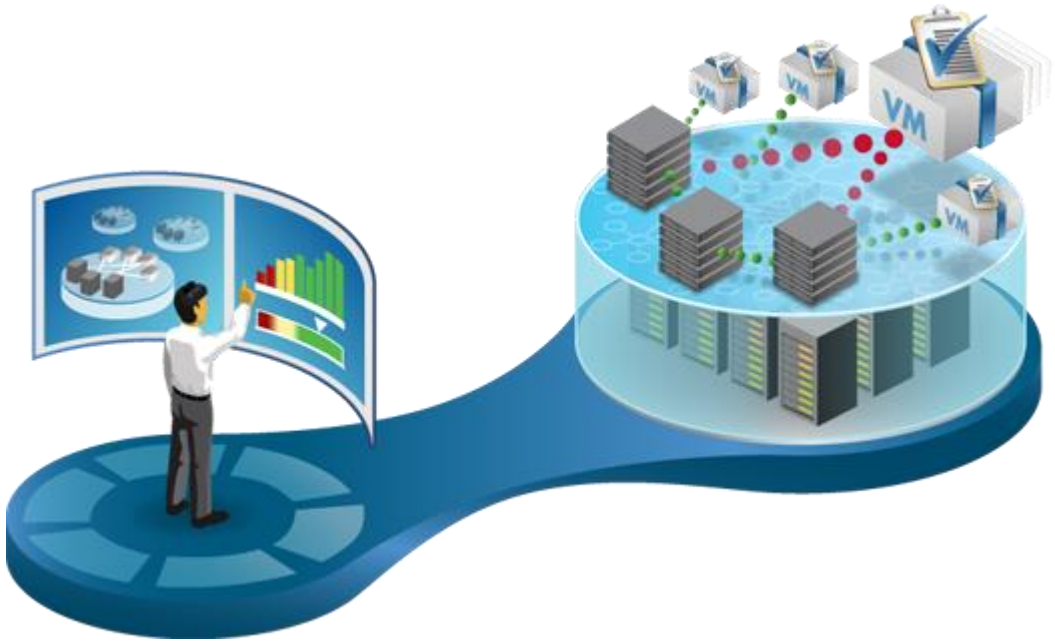
d) Gestión de TI

Gestión de TI

- Estructura de relaciones y procesos diseñados y ejecutados para dirigir y controlar la tecnología de información, sus riesgos asociados y su vinculación con las estrategias y objetivos del negocio.

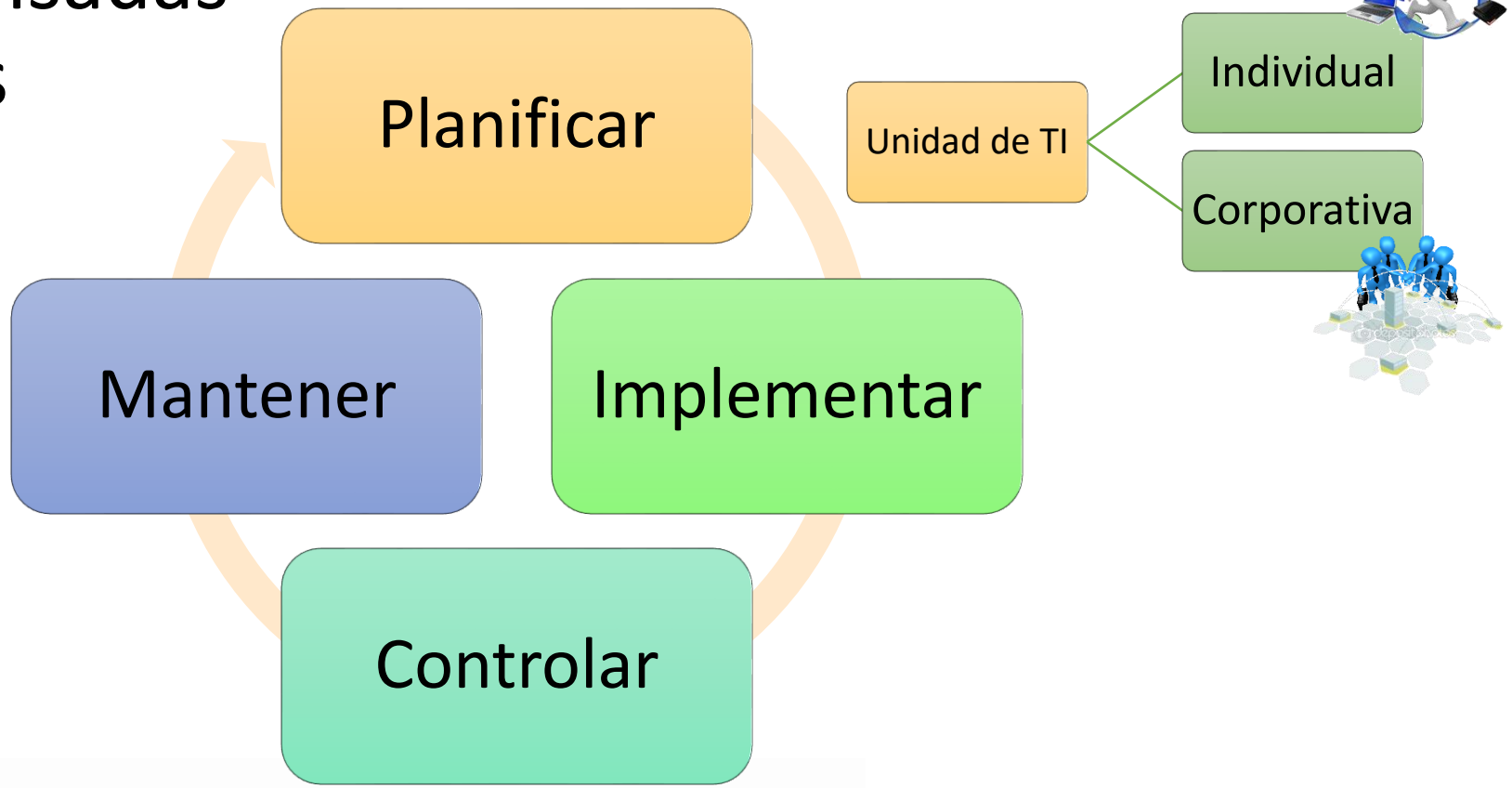
Marco de Gestión de TI

- Conjunto de **procesos destinados** a *gestionar* TI.
- Gestión **integral** de **riesgos** tecnológicos.
- Considerando el principio de proporcionalidad y particularidades.



Marco de Gestión de TI

Entidades supervisadas son responsables



SUGEF SUPEN SUGESE SUGEVAL

Marco de gestión de TI

Debe formularse considerando las particularidades de cada entidad supervisada.

- Naturaleza
- Complejidad
- Modelo de negocio
- Volumen de operaciones
- Criticidad de procesos
- Dependencia tecnológica
- Cualquier otro (Entidad o Superintendencia)

Determinado a través del perfil tecnológico

Marco de Gestión de TI

- El análisis de procesos debe ser realizado mediante un estudio técnico.

Procesos de Gobierno de TI Empresarial

Evaluar, Orientar y Supervisar

- 1.1 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno
- 1.2 Asegurar la Entrega de Beneficios
- 1.3 Asegurar la Optimización del Riesgo
- 1.4 Asegurar la Optimización de los Recursos
- 1.5 Asegurar la Transparencia hacia las Partes Interesadas

Alinear, Planificar y Organizar

- 2.1 Gestionar el Marco de Gestión de TI
- 2.2 Gestionar la Estrategia
- 2.3 Gestionar la Arquitectura Empresarial
- APO04 No aplica
- 2.4 Gestionar el portafolio de Servicios
- 2.5 Gestionar el presupuesto y los costos
- 2.6 Gestionar los recursos humanos
- 2.7 Gestionar las relaciones entre TI y el negocio
- 2.8 Gestionar los acuerdos de niveles de servicio
- 2.9 Gestionar los servicios de los proveedores de TI
- 2.10 Gestionar la Calidad
- 2.11 Gestionar el riesgo de TI
- 2.12 Gestionar la seguridad

Construir, Adquirir e Implementar

- 3.1 Gestionar programas y proyectos
- 3.2 Gestionar la definición de requerimientos
- 3.3 Gestionar la identificación y construcción de soluciones
- 3.4 Gestionar la disponibilidad y capacidad
- BAIA06 No aplica
- 3.5 Gestionar los cambios
- 3.6 Gestionar la aceptación del cambio y la transición
- BAIA08 No aplica
- 3.7 Gestionar los activos de TI
- 3.8 Gestionar la configuración

Entregar, dar Servicio y Soporte

- 4.1 Gestionar las operaciones
- 4.2 Gestionar peticiones incidentes servicio
- 4.3 Gestionar los problemas
- 4.4 Gestionar la continuidad
- 4.5 Gestionar servicios de seguridad de la información
- 4.6 Gestionar controles de proceso de negocio

Supervisar, Evaluar y Valorar

- 5.1 Supervisar, evaluar y valorar el rendimiento y la conformidad
- 5.2 Supervisar, evaluar y valorar el sistema de control interno
- 5.3 Supervisar, evaluar y valorar la conformidad con los requerimientos externos

Procesos para la Gestión de la TI Empresarial

3. Disposiciones del Reglamento

Anexo 1: Procesos del Marco de Gestión de TI para SUGEVAL, SUPEN y SUGESE

AÑO 1 (11 procesos)	AÑO 2 (7 procesos)	AÑO 3 (7 procesos)	AÑO 4 (6 procesos)	AÑO 5 (3 procesos)
•1.1. Asegurar el establecimiento y mantenimiento marco gobierno. •1.2. Asegurar Entrega Beneficios. •1.3. Asegurar la Optimización Riesgo. •1.4. Asegurar Optimización Recursos. •1.5. Asegurar la Transparencia hacia las Partes Interesadas. •2.1. Gestionar Marco de Gestión TI. •2.2. Gestionar la Estrategia. •2.8. Gestionar los acuerdos servicio. •2.9. Gestionar los Proveedores. •3.1.Gestión de Programas-Proyectos •4.2. Gestionar Peticiones e Incidentes de Servicio.	• 2.11. Gestionar el Riesgo. • 2.12. Gestionar Seguridad • 3.5. Gestionar Cambios. • 4.4. Gestionar Continuidad • 4.5. Gestionar Servicios de Seguridad. • 4.6. Gestionar Controles de Proceso de Negocio. • 5.2. Supervisar, Evaluar y Valorar el Sistema de Control Interno.	• 2.5. Gestionar Presupuesto y Costos. • 3.3. Gestionar Identificación y Construcción Soluciones • 3.4. Gestionar disponibilidad y Capacidad. • 3.7. Gestionar los Activos. • 3.8. Gestionar la Configuración. • 4.1. Gestionar Operaciones. • 4.3. Gestionar Problemas.	• 2.3. Gestionar Arquitectura Empresarial. • 2.4. Gestionar el Portafolio. • 2.6. Gestionar los Recursos Humanos. • 2.7. Gestionar las relaciones. • 3.2. Gestionar la Definición de Requisitos. • 3.6. Gestionar la Aceptación del Cambio y Transición.	• 2.10. Gestionar la Calidad. • 5.1. Supervisar, Evaluar y Valorar el Rendimiento . • 5.3. Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.

SUGEF Superintendencia General de Entidades Financieras Costa Rica · SUGE · SUPEN Superintendencia de Pensiones · SUGESE · SUGESE Superintendencia General de Seguros República de Costa Rica · SUGEVAL Superintendencia General de Valores

3. Disposiciones del Reglamento

Anexo 1: Procesos del Marco de Gestión de TI para SUGEF

A la entrada en vigencia (18 procesos)	AÑO 1 (6 procesos)	AÑO 2 (6 procesos)	AÑO 3 (4 procesos)
•2.1. Gestionar el Marco de Gestión TI. •2.2. Gestionar la Estrategia. •2.5. Gestionar el Presupuesto y los Costos. •2.8. Gestionar los acuerdos de servicio. •2.9. Gestionar los Proveedores. •2.11. Gestionar el Riesgo. •2.12. Gestionar la Seguridad. •3.1. Gestión de Programas y Proyectos. •3.3. Gestionar Identificación y Construcción Soluciones. •3.4. Gestionar la Disponibilidad y la Capacidad. •3.5. Gestionar los Cambios. •3.8. Gestionar la Configuración. •4.1. Gestionar Operaciones. •4.2. Gestionar Peticiones e Incidentes Servicio. •4.3. Gestionar Problemas. •4.4. Gestionar la Continuidad. •4.5. Gestionar Servicios de Seguridad. •5.2. Supervisar, Evaluar y Valorar Sistema Control Interno.	• 1.1. Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno. • 1.2. Asegurar la Entrega de Beneficios. • 1.3. Asegurar la Optimización del Riesgo. • 1.4. Asegurar la Optimización de Recursos. • 1.5. Asegurar la Transparencia hacia las Partes interesadas. • 4.6. Gestionar Controles de Proceso de Negocio.	• 2.3. Gestionar la Arquitectura Empresarial. • 2.4. Gestionar el Portafolio. • 2.6. Gestionar los Recursos Humanos. • 3.2. Gestionar la Definición de Requisitos. • 3.6. Gestionar la Aceptación del Cambio y la Transición. • 3.7. Gestionar los Activos.	• 2.7. Gestionar las relaciones. • 2.10. Gestionar la calidad. • 5.1. Supervisar, Evaluar y Valorar el Rendimiento. • 5.3. Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.

SUGEF Superintendencia General de Entidades Financieras Costa Rica · SUGE · SUPEN Superintendencia de Pensiones · SUGESE · SUGESE Superintendencia General de Seguros República de Costa Rica · SUGEVAL Superintendencia General de Valores

Marco de gestión

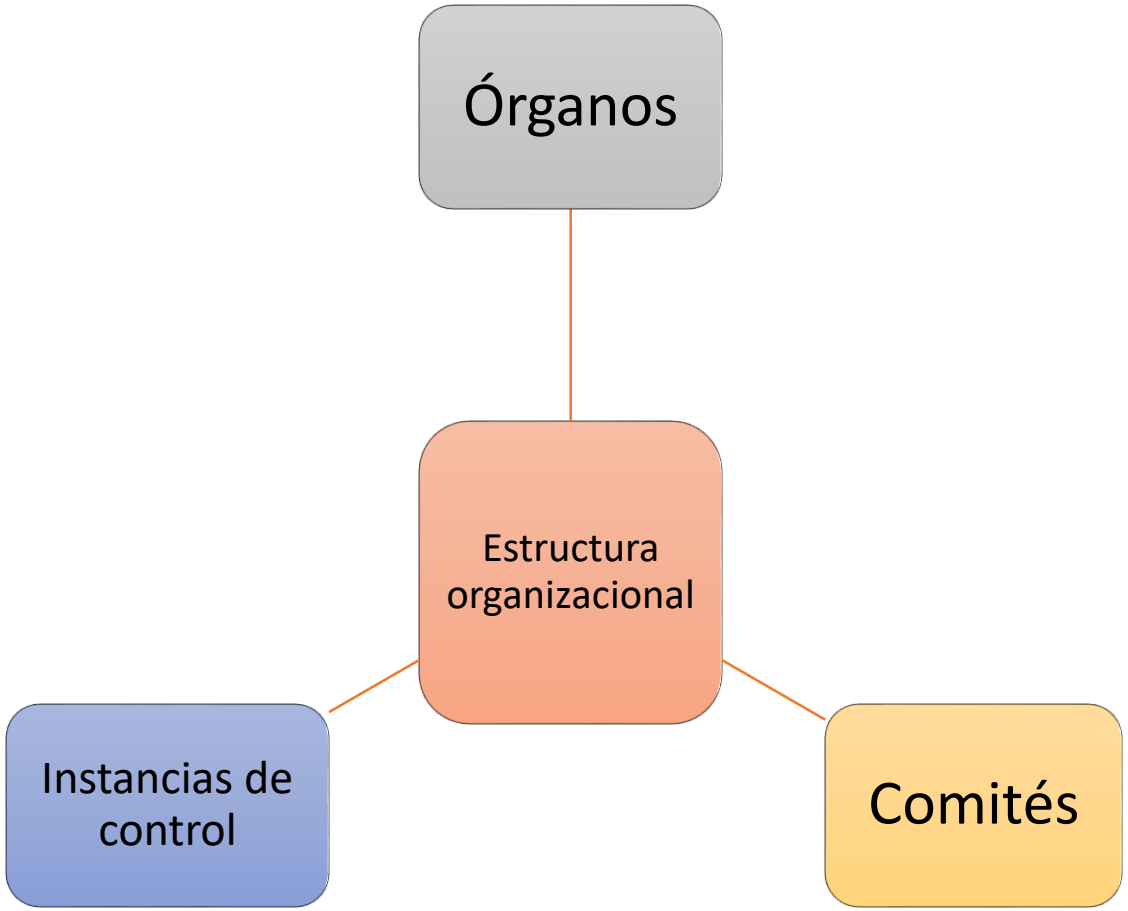
Validación

- La superintendencia mediante resolución razonada puede:
  - **Validar** o **incluir** procesos en el marco de gestión de TI.
  - Criterios:
    - Según necesidades de supervisión.
    - El riesgo identificado para la entidad (nuevos).
    - El marco de gestión de TI establecido por la entidad no es acorde a sus particularidades.

Gestión de TI

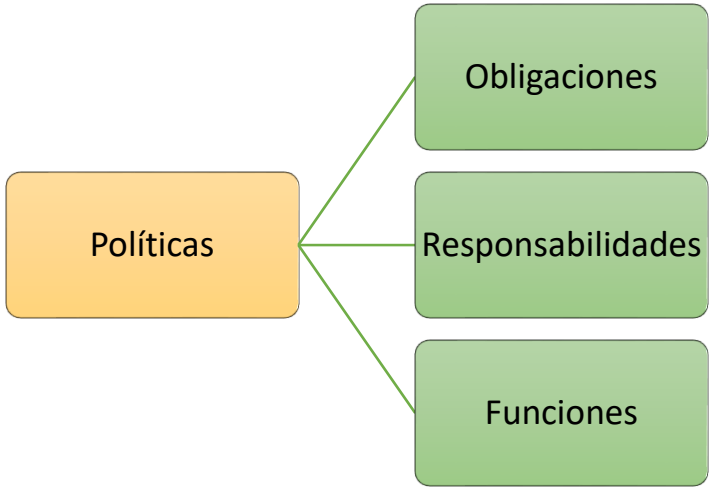
Principio de proporcionalidad

Entidades	Elementos
SUGESE	Dependencia tecnológica y complejidad de las operaciones
SUGEVAL	Criticidad de los procesos
SUPEN	Modelo de negocio
SUGEF	Naturaleza



Gestión de TI

Mecanismos de control para las estructuras de administración de TI

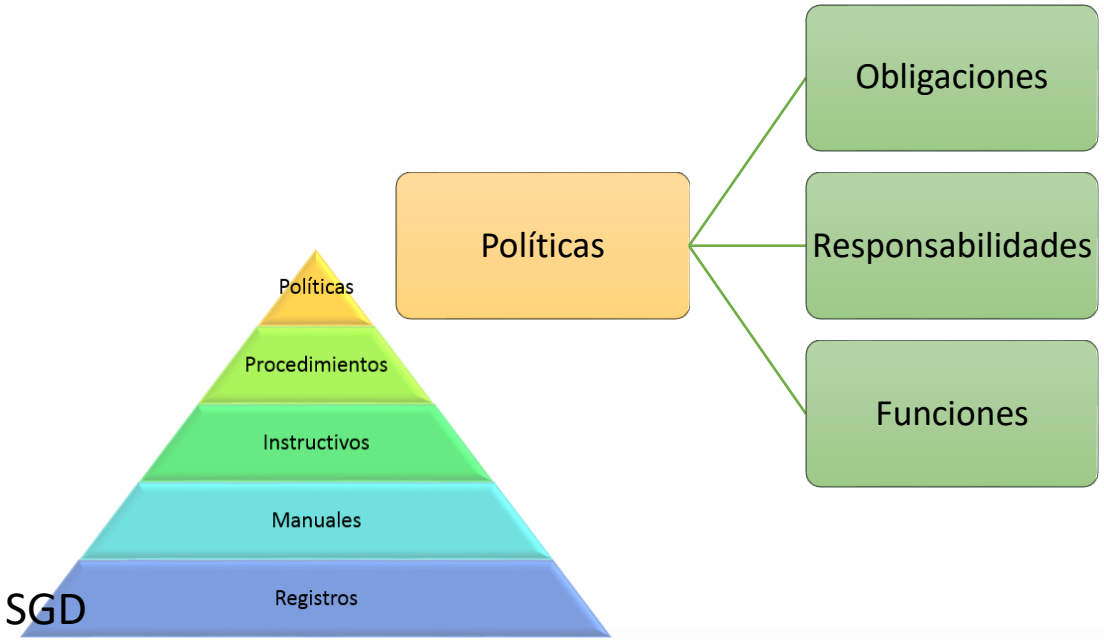


SGD

- Órgano de Dirección
  - Aprobar el marco de gestión de TI
  - Involucrar al personal
    - Integrantes Junta Directiva
    - Alta Gerencia
    - Líder de Informática
    - Líder de Riesgos
  - Firma de auditores (Comité)
  - Aprobar políticas de gestión
  - Informes de auditoría

Gestión de TI

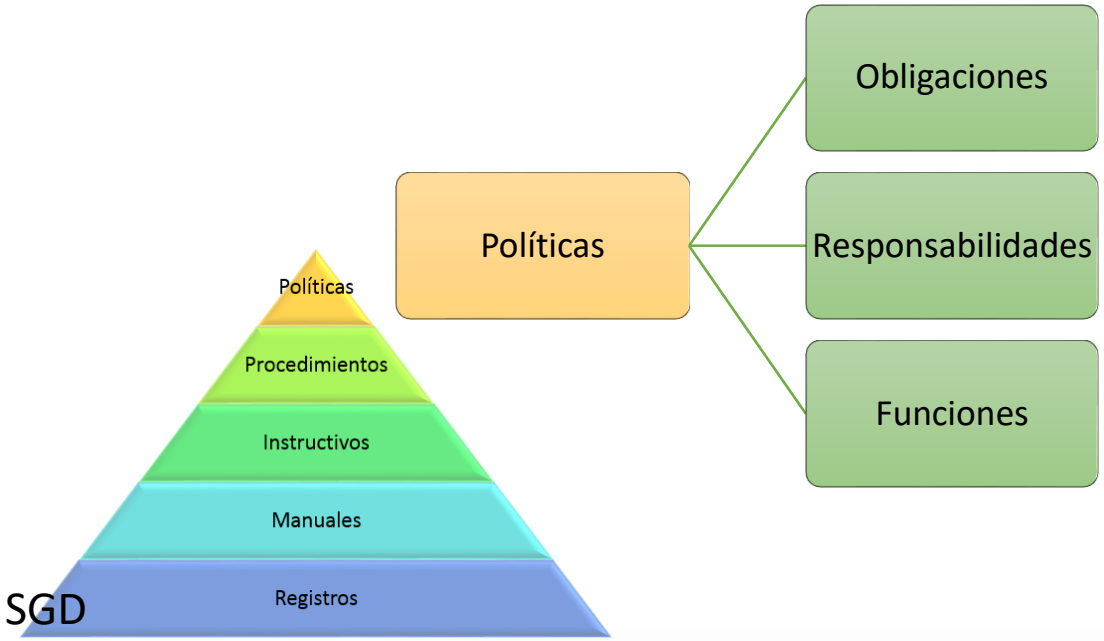
Mecanismos de control para las estructuras de administración de TI



- Alta Gerencia
  - Implementar marcos de control.
  - Proponer los recursos necesarios implementación del marco de TI.
  - Proponer firma de auditores externos
  - Controlar.
    - Las políticas y procedimientos de gestión de TI.
  - Designar responsables de implementación.
  - Atender requerimientos del Supervisor.

Gestión de TI

Mecanismos de control para las estructuras de administración de TI



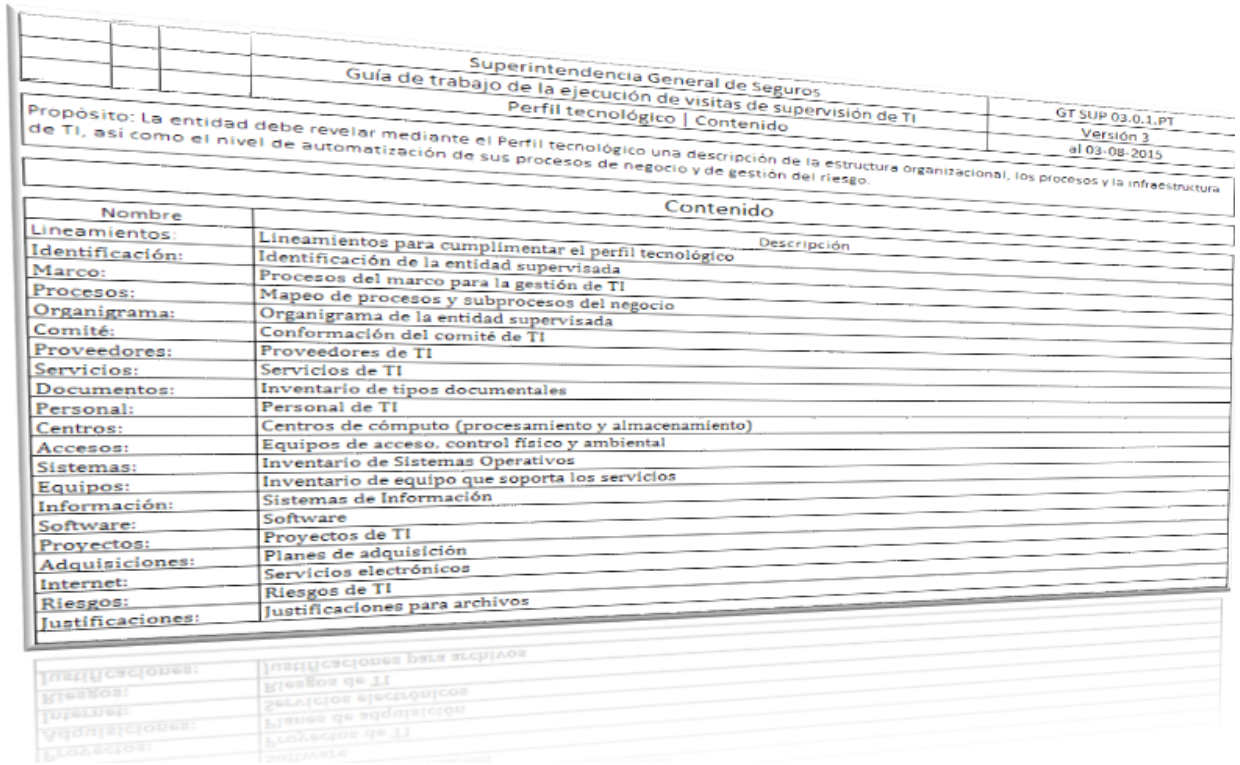
SGD

- Comité de TI
  - Velar por cumplimiento de procesos de TI
  - Asesor en formulación del las estrategias y metas de TI y su cumplimento.
  - Proponer políticas con base marco de gestión.
  - Recomendar prioridades de inversión de TI.
  - Proponer niveles de tolerancia la riesgo de TI.
  - Velar por que la gerencia gestione el riesgo de TI en concordancia con el marco aprobado.
  - Analizar y dar seguimiento al Plan de acción.

Perfil tecnológico

e) Perfil

Perfil tecnológico



Superintendencia General de Seguros

Guía de trabajo de la ejecución de visitas de supervisión de TI | GT SUP 03.0.1.PT

Perfil tecnológico | Contenido | Versión 3 al 03-08-2015

Propósito: La entidad debe revelar mediante el Perfil tecnológico una descripción de la estructura organizacional, los procesos y la infraestructura de TI, así como el nivel de automatización de sus procesos de negocio y de gestión del riesgo.

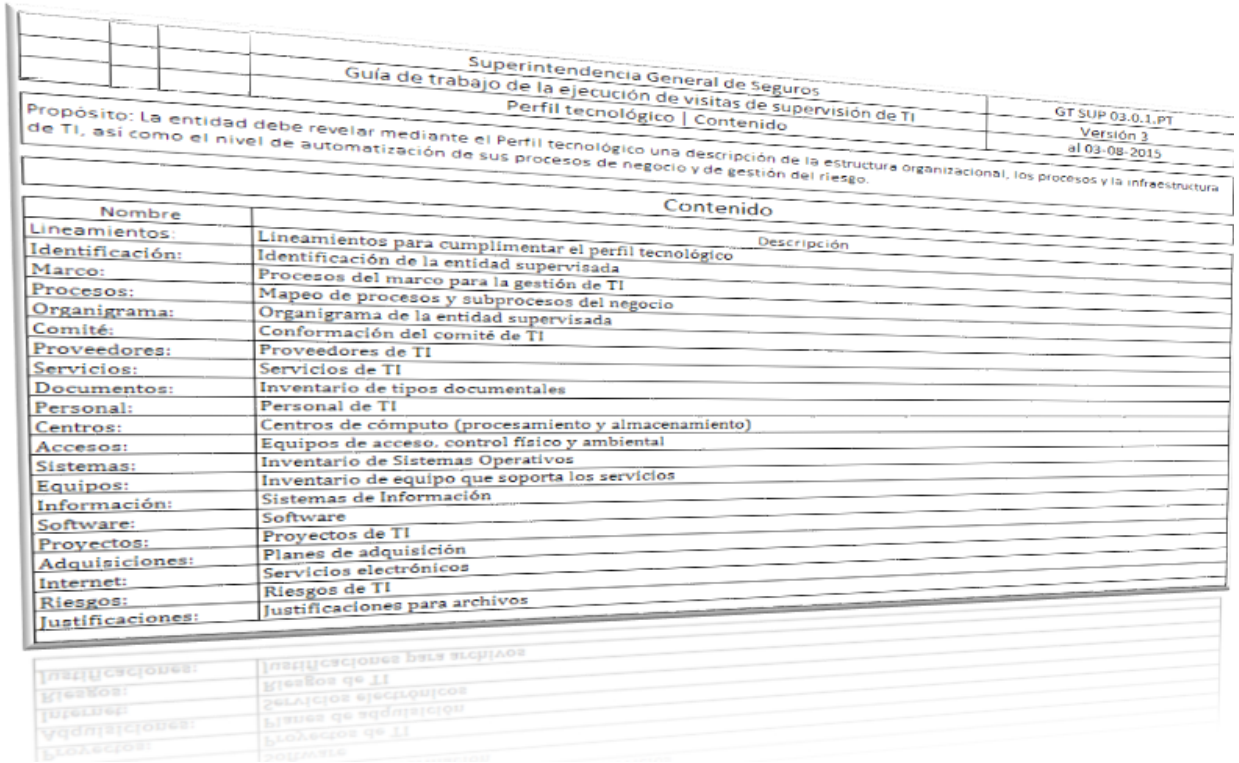
Nombre	Contenido
	Descripción
Lineamientos:	Lineamientos para cumplimentar el perfil tecnológico
Identificación:	Identificación de la entidad supervisada
Marco:	Procesos del marco para la gestión de TI
Procesos:	Mapeo de procesos y subprocesos del negocio
Organigrama:	Organigrama de la entidad supervisada
Comité:	Conformación del comité de TI
Proveedores:	Proveedores de TI
Servicios:	Servicios de TI
Documentos:	Inventario de tipos documentales
Personal:	Personal de TI
Centros:	Centros de cómputo (procesamiento y almacenamiento)
Accesos:	Equipos de acceso, control físico y ambiental
Sistemas:	Inventario de Sistemas Operativos
Equipos:	Inventario de equipo que soporta los servicios
Información:	Sistemas de Información
Software:	Software
Proyectos:	Proyectos de TI
Adquisiciones:	Planes de adquisición
Internet:	Servicios electrónicos
Riesgos:	Riesgos de TI
Justificaciones:	Justificaciones para archivos

- Estructura organizacional
- Los procesos
- La infraestructura de TI
- Nivel de automatización de sus procesos de negocio y de gestión del riesgo.

Responsabilidad de la entidad elaborar y mantener actualizado su perfil tecnológico.

SUGEF SUPEN SUGESE SUGEVAL

Perfil tecnológico



Superintendencia General de Seguros

Guía de trabajo de la ejecución de visitas de supervisión de TI

Perfil tecnológico | Contenido

GT SUP 03.0.1_PT
Versión 3
al 03-08-2015

Propósito: La entidad debe revelar mediante el Perfil tecnológico una descripción de la estructura organizacional, los procesos y la infraestructura de TI, así como el nivel de automatización de sus procesos de negocio y de gestión del riesgo.

Contenido	
Nombre	Descripción
Lineamientos:	Lineamientos para cumplimentar el perfil tecnológico
Identificación:	Identificación de la entidad supervisada
Marco:	Procesos del marco para la gestión de TI
Procesos:	Mapeo de procesos y subprocesos del negocio
Organigrama:	Organigrama de la entidad supervisada
Comité:	Conformación del comité de TI
Proveedores:	Proveedores de TI
Servicios:	Servicios de TI
Documentos:	Inventario de tipos documentales
Personal:	Personal de TI
Centros:	Centros de cómputo (procesamiento y almacenamiento)
Accesos:	Equipos de acceso, control físico y ambiental
Sistemas:	Inventario de Sistemas Operativos
Equipos:	Inventario de equipo que soporta los servicios
Información:	Sistemas de Información
Software:	Software
Proyectos:	Proyectos de TI
Adquisiciones:	Planes de adquisición
Internet:	Servicios electrónicos
Riesgos:	Riesgos de TI
Justificaciones:	Justificaciones para archivos

Unidad de TI corporativa

- Debe remitirse un único perfil.
- Coordinar que ese perfil tecnológico se ajuste al marco de gestión de TI aprobado por cada Superintendencia.
- El marco de gestión de TI puede ser integrado
- Se deben diferenciar aquellos procesos y estándares que son particulares de cada entidad supervisada

Tipo de gestión

f) Tipo de gestión

Tipo de gestión de TI

- Las entidades supervisadas pueden solicitar que su gestión de TI sea **tipificada** como **corporativa** cuando la unidad de TI **provee servicios a todas las entidades integrantes** del grupo o conglomerado financiero.

Tipo de gestión de TI

- Los superintendentes pueden solicitar información adicional para complementar la información proporcionada en el perfil tecnológico.

Tipo de gestión de TI

- Las Superintendencias deben resolver dicha solicitud en el **plazo de veinte días** hábiles contados a partir de la recepción de la solicitud y su documentación completa.

Tipo de gestión de TI

Solicitud

- **La entidad** debe realizar la solicitud **indiciando una justificación** debidamente sustentada **del por qué se considera que el modelo de la gestión de TI es corporativa**.

Cora Amalia Castilla Madrid
PRESIDENTA MUNICIPAL
H. AYUNTAMIENTO DE OTHÓN P. BLANCO

Cd. Chetumal, Q.R. 20 de abril del 2007

SEÑOR
VICENTE RAMÓN FERRER
EDITORIAL OX

PM/304/07

El Honorable Ayuntamiento Othón P. Blanco que me honro presidir agradece y acepta el Premio OX 2007, otorgado por su editorial al portal de nuestro municipio en la categoría de Organismos y Gobierno.

Creamos www.opb.gob.mx con el propósito de abrir Chetumal y Othón P. Blanco al mundo, pero sobre todo a quienes con su trabajo y esfuerzo contribuyen a su progreso y desarrollo. Nos esforzamos en que la casa de todos los othonenses que es el municipio, esté cada vez más presente en el quehacer diario de nuestros ciudadanos e incluso de aquellos que, sin vivir aquí, quieran conocernos mejor.

Este reconocimiento estimula nuestro trabajo y nos compromete aún más, al saber que nuestra labor ha trascendido fronteras mexicanas.

ATENTAMENTE

SUGEF SUPEN SUGESE SUGEVAL

Tipo de gestión de TI

Cora Amalia Castilla Madrid
PRESIDENTA MUNICIPAL
H. AYUNTAMIENTO DE OTHÓN P. BLANCO

Cd. Chetumal, Q.R. 20 de abril del 2007

SEÑOR
VICENTE RAMÓN FERRER
EDITORIAL OX

PM/304/07

El Honorable Ayuntamiento Othón P. Blanco que me honro presidir agradece y acepta el Premio OX 2007, otorgado por su editorial al portal de nuestro municipio en la categoría de Organismos y Gobierno.

Creamos www.opb.gob.mx con el propósito de abrir Chetumal y Othón P. Blanco al mundo, pero sobre todo a quienes con su trabajo y esfuerzo contribuyen a su progreso y desarrollo. Nos esforzamos en que la casa de todos los othonenses que es el municipio, esté cada vez más presente en el quehacer diario de nuestros ciudadanos e incluso de aquellos que, sin vivir aquí, quieran conocernos mejor.

Este reconocimiento estimula nuestro trabajo y nos compromete aún más, al saber que nuestra labor ha trascendido fronteras mexicanas.

ATENTAMENTE

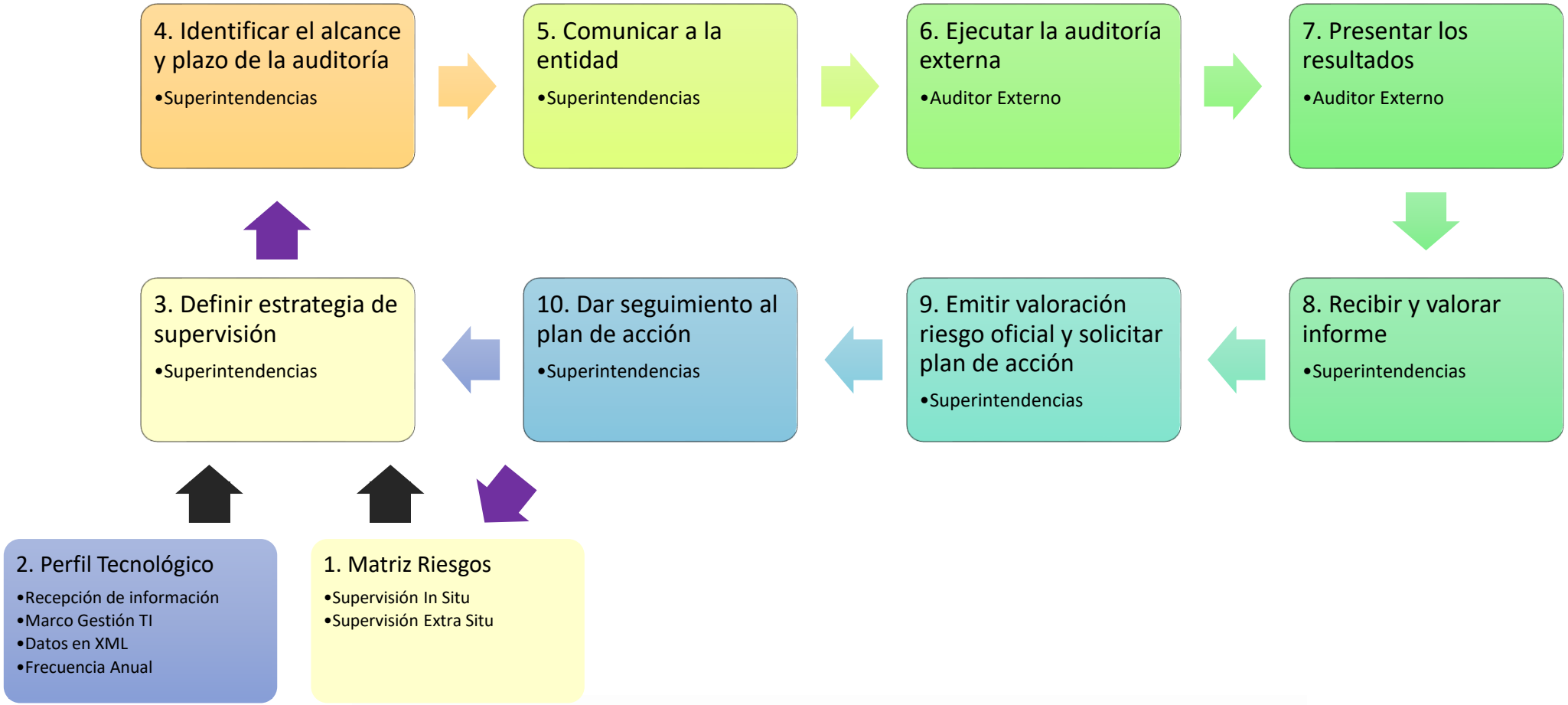
Requisitos

a. Gestión de recursos.
b. Formulación de políticas y procedimientos.
c. Aspectos financieros.
d. Esquema de coordinación.
e. Aspectos de control.
f. Plataforma tecnológica.
g. Servicios de TI brindados por terceros.
    i. Contratos.
    ii. Referencias de la aprobación del contrato entre la entidad y el proveedor que presta el servicio.

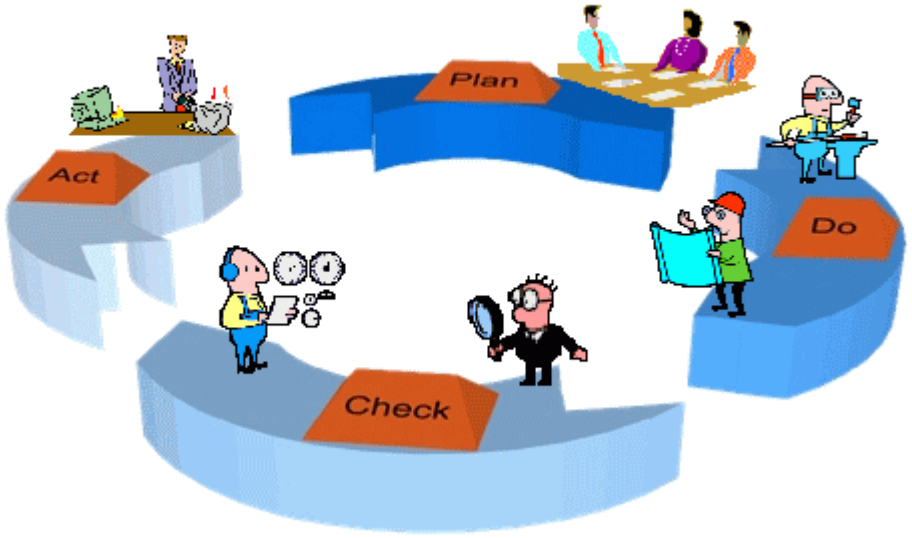
Proceso del reglamento

g) proceso

Proceso de la implementación de la norma



SUGEF SUPEN SUGESE SUGEVAL



Proceso de auditoría

h) Auditoría externa, resultado, reporte, planes de acción, prórrogas y calificación

Auditoría externa de TI

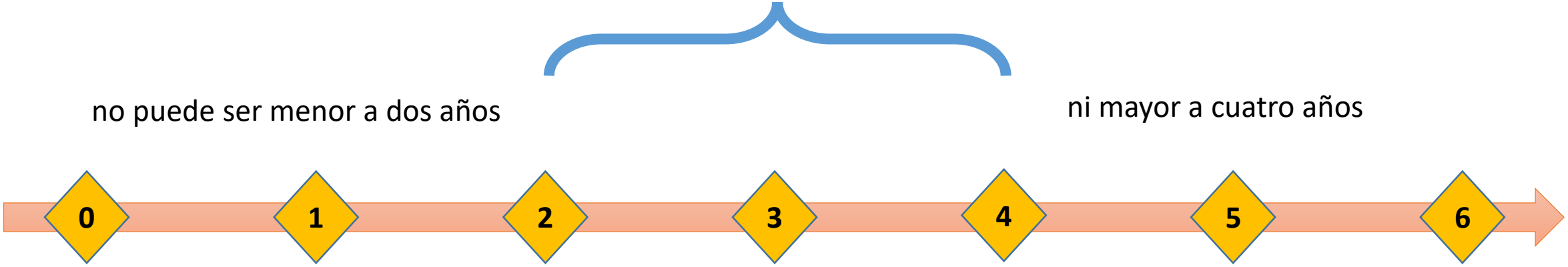
- **El supervisor solicitará** a las **entidades** supervisadas la **contratación de una auditoría externa de TI.**
- Sobre el marco de gestión de TI y su aplicación, según lo que se defina en el alcance de la auditoría.

Auditoría externa de TI

- Criterios para la ejecución
  - Normas de Auditoría y aseguramiento de SI emitidas por ISACA

Auditoría externa de TI

- A partir de la primera auditoría, el intervalo entre una y otra solicitud

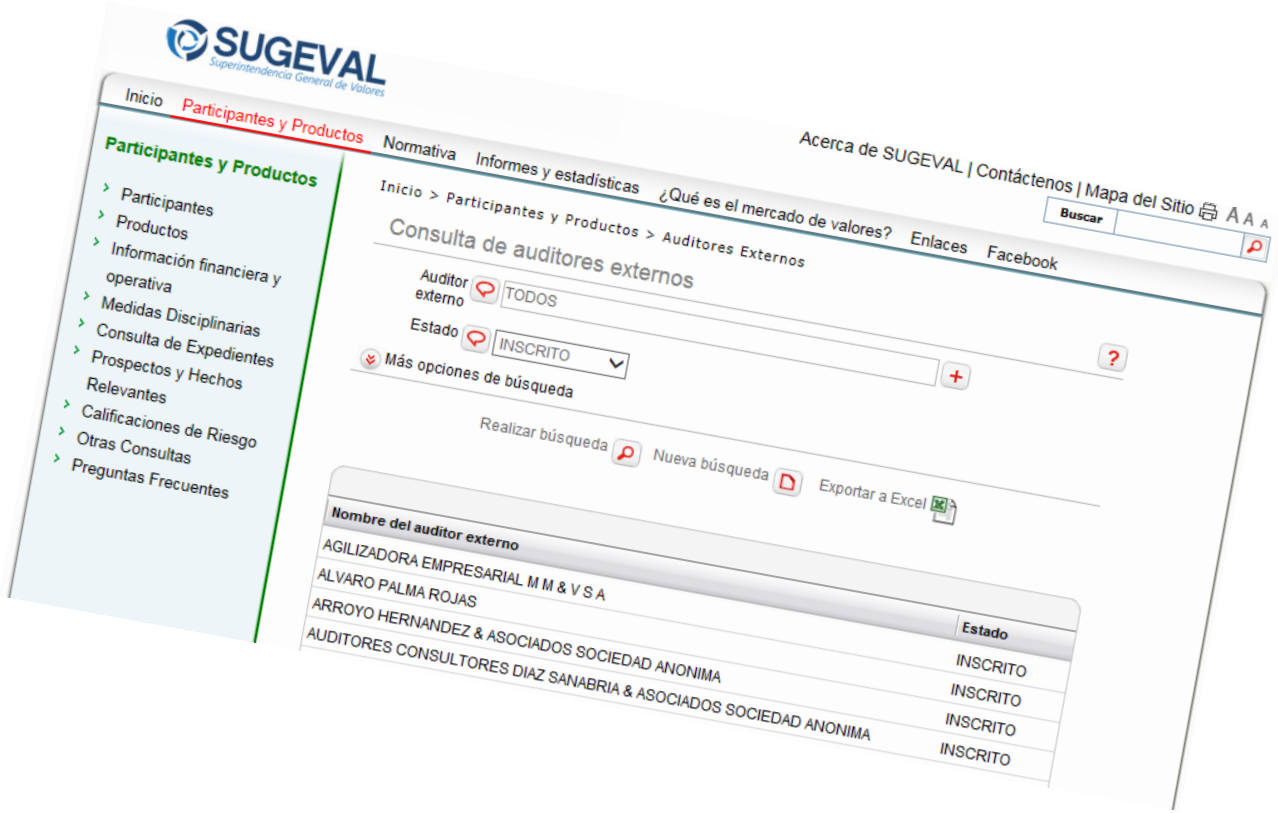


Auditoría externa de TI

- El contrato con el auditor externo debe incluir cláusula que obligue a éste a entregar al supervisor, copia de la información.
- En un plazo máximo de **cinco días hábiles** contados a partir de recibida la solicitud de entrega.

Auditoría externa de TI

- Auditor inscrito en el registro de auditores elegibles.
- Sujeto a requisitos de idoneidad.

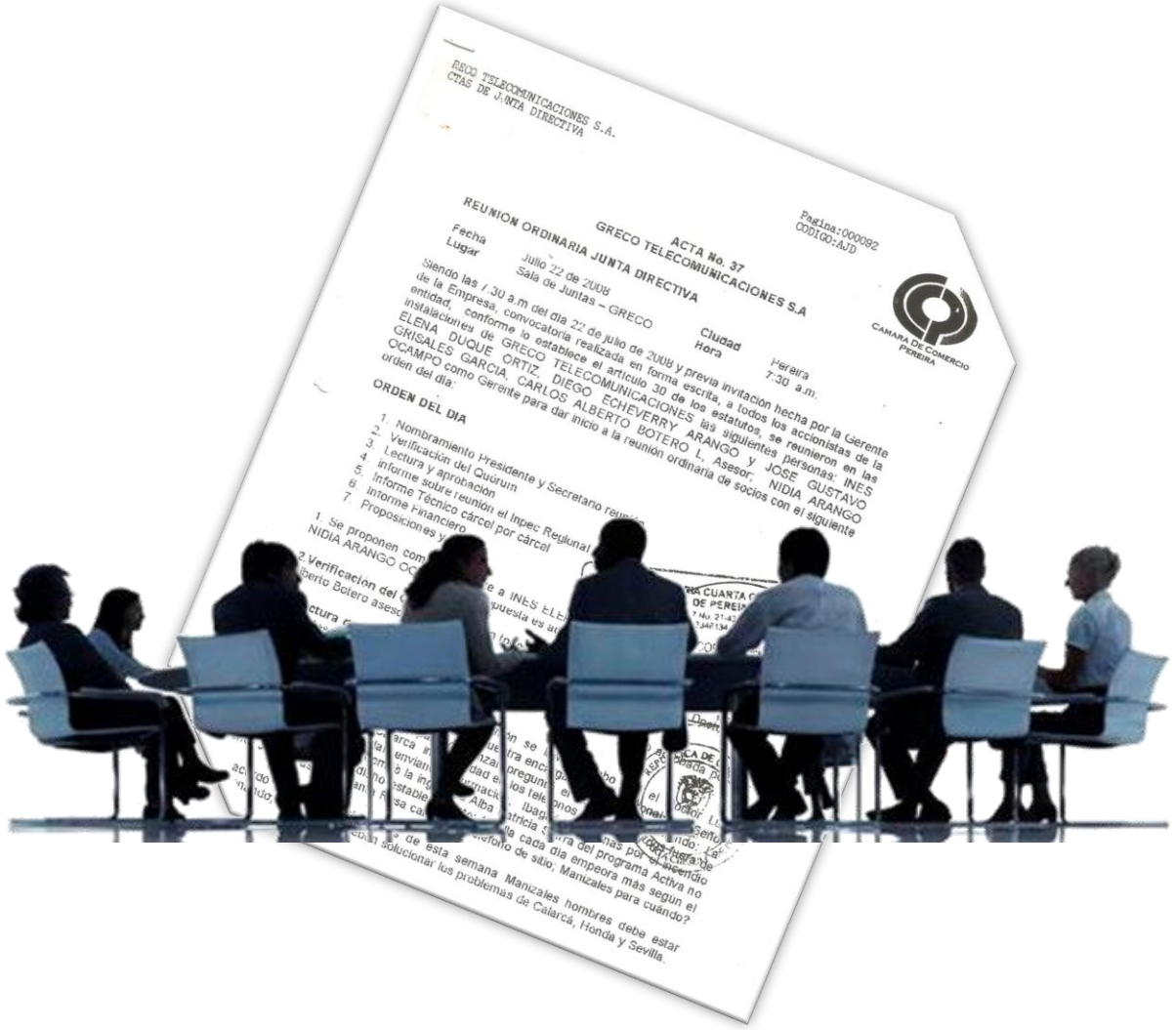


Auditoría externa de TI

- **Unidad de TI Corporativa**
  - Le corresponde a los órganos de dirección asegurarse y coordinar que el alcance de la auditoría incluya todo aquello que corresponde a cada una de las entidades supervisadas.

Auditoría externa de TI

- Auditoría externa corporativa.
  - Los **órganos directivos** de las entidades supervisadas deben **dejar constancia de la aprobación del contrato de servicios.**
  - Los contratos debe cumplir con todos los requisitos establecidos en las regulaciones vigentes**.**



Alcance y plazo de la auditoría externa de TI

Alcance

- Lo establece el supervisor mediante la definición de al menos los siguientes aspectos:
  - Procesos y objetivos de control a evaluar, con base en el marco de gestión de TI aplicable en el momento de la solicitud de la auditoría externa de TI.
  - Entidades supervisadas y áreas de negocio a considerar en cada proceso.
  - Servicios de TI suministrados por proveedores de TI.
  - Periodo de cobertura.

Productos entregables de la auditoría externa de TI

Productos entregables

a) El informe de la auditoría externa de TI según el formato establecido en los Lineamientos Generales.

b) La matriz de evaluación de la los procesos auditados de TI según lo establecido en los Lineamientos Generales y los riesgos asociados, y

c) Copia del acuerdo del órgano directivo de la entidad, en el cual aprueba el informe de la auditoría externa de TI.

Productos entregables de la auditoría externa de TI

Matriz de evaluación 

a) Contiene los criterios que serán evaluados para cada proceso del marco de gestión,

b) La entidad supervisada debe entregar la matriz de evaluación de la gestión de TI al Auditor externo de TI.

Resultados de la auditoría externa de TI

Presentación de los resultados

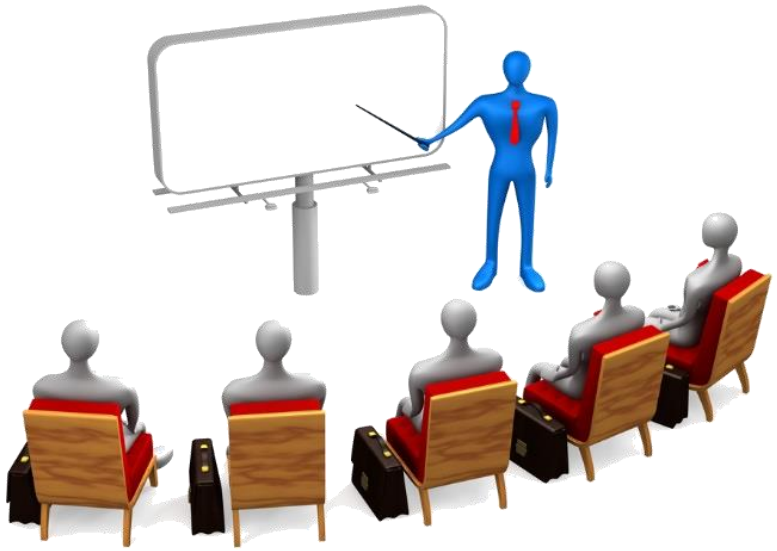
a) Las entidades realizarán una convocatoria para reunión de salida.

b) El auditor debe seguir los **Lineamientos Generales para los contenidos mínimos** de la presentación.

Resultados de la auditoría externa de TI

Presentación de los resultados

El auditor externo de TI debe presentar los resultados.



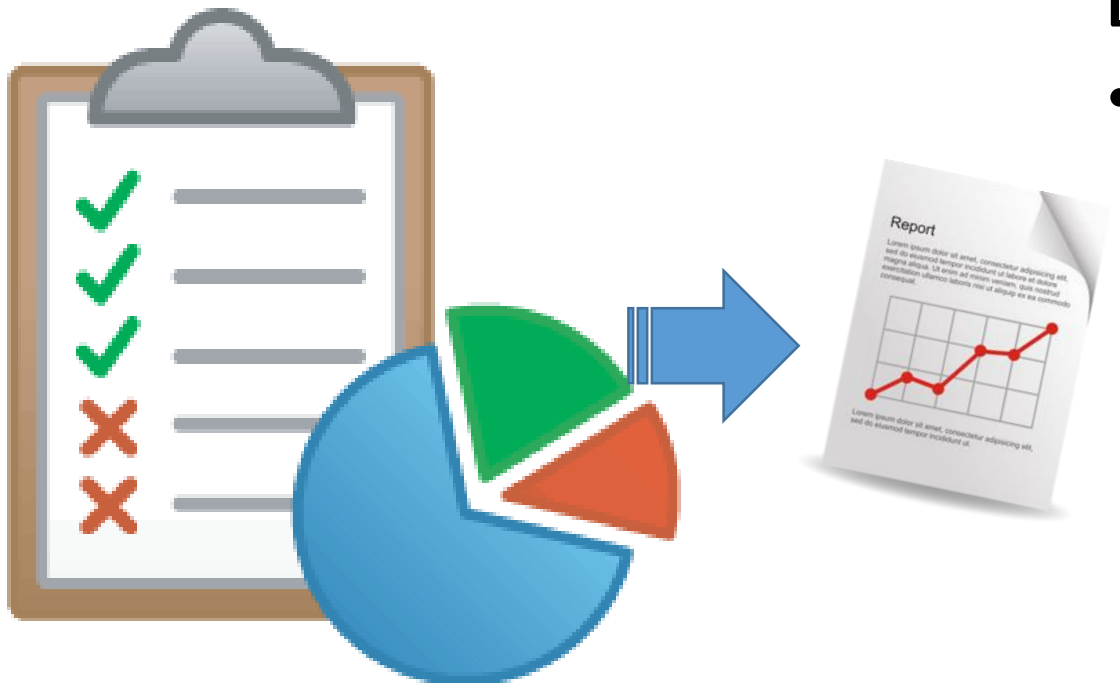
Participantes

a) Los colaboradores que estimen las superintendencias.
b) El Gerente General.
c) El responsable de la unidad de TI.
d) El auditor interno.
e) El presidente del comité de vigilancia(cuando corresponda).

Reporte de supervisión

a) La superintendencia realizará un informe de supervisión.
   a) Los resultados la auditoría externa.
   b) Los resultados de supervisión realizada directamente por la superintendencia.

Reporte de supervisión



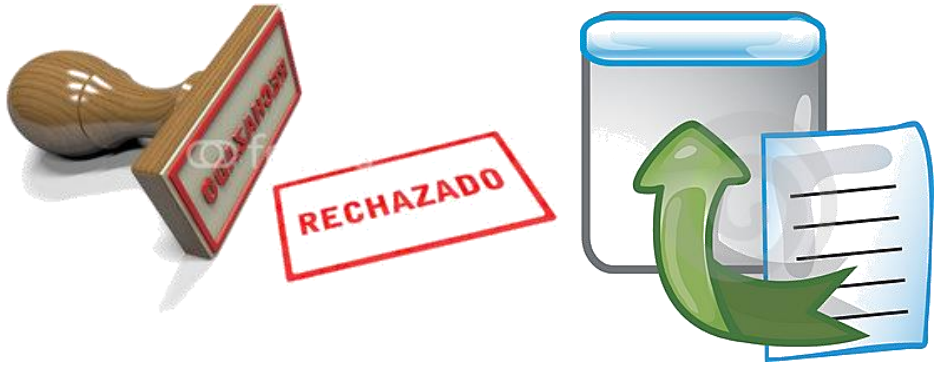
Discrepancias

- Cuando haya una auditoría externa y el o los supervisores se aparten de la opinión emitida por el auditor de TI debe incluirse la debida justificación.

Reporte de supervisión

Inadmisibilidad de los productos

- El supervisor puede declarar **inadmisible** los productos.
- Cuando incumplan las disposiciones establecidas en el Reglamento o sus Lineamientos Generales.



Reporte de supervisión

Revaloración de los productos

a) **La entidad** supervisada debe **remitir los productos entregables corregidos**.

b) Se debe realizar la reunión de salida.

c) El supervisor en caso de determinar hallazgos y riesgos, en la nota de remisión requerirá un plan de acción.

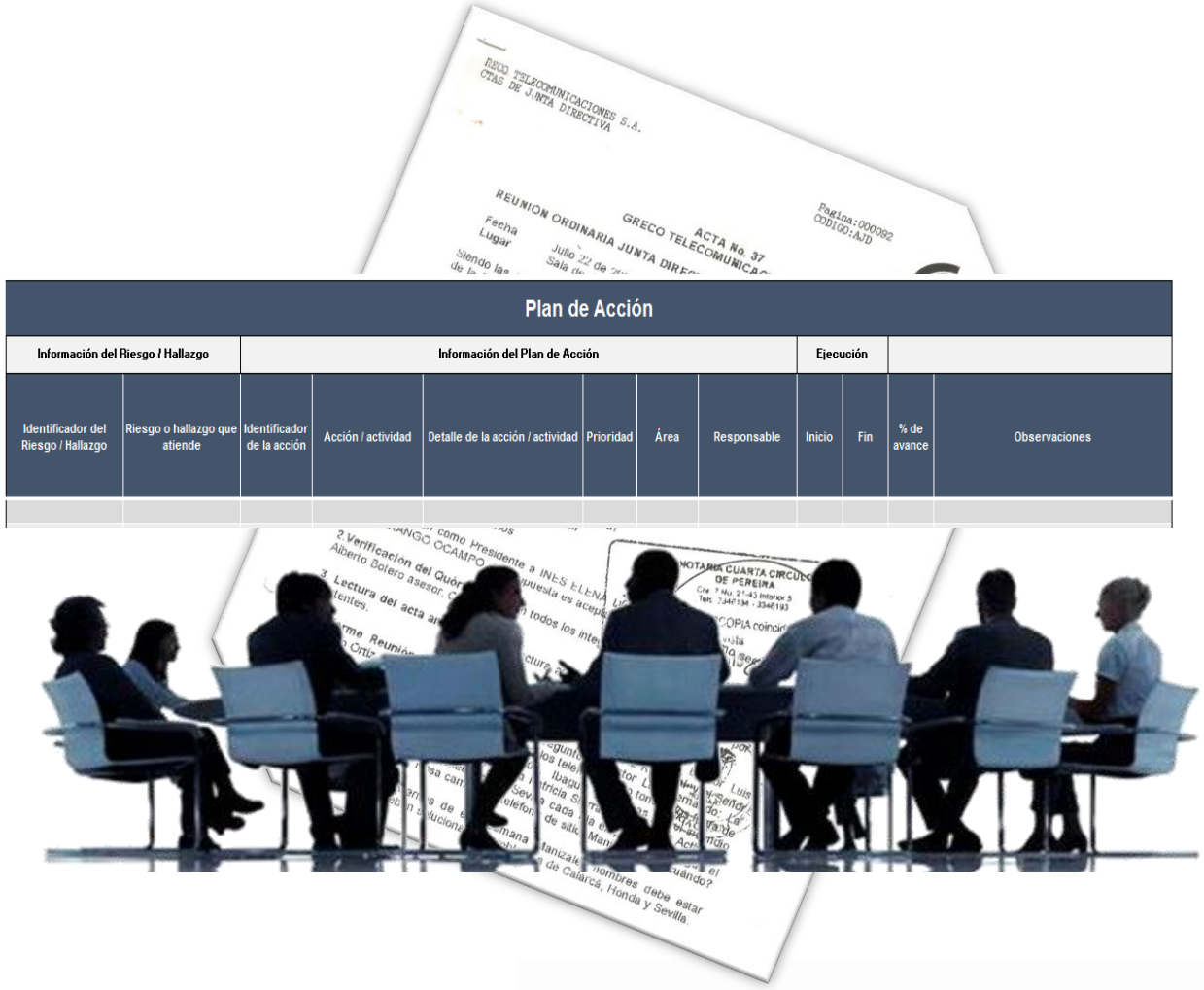
Plan de acción

El plan

a) La entidad supervisada debe presentar el plan de acción con el formato y plazo establecidos en los Lineamientos Generales.

Plan de Acción											
Información del Riesgo / Hallazgo		Información del Plan de Acción						Ejecución			
Identificador del Riesgo / Hallazgo	Riesgo o hallazgo que atiende	Identificador de la acción	Acción / actividad	Detalle de la acción / actividad	Prioridad	Área	Responsable	Inicio	Fin	% de avance	Observaciones

Plan de acción



Aprobación del plan

a) Aprobado por el órgano de dirección de la entidad supervisada.

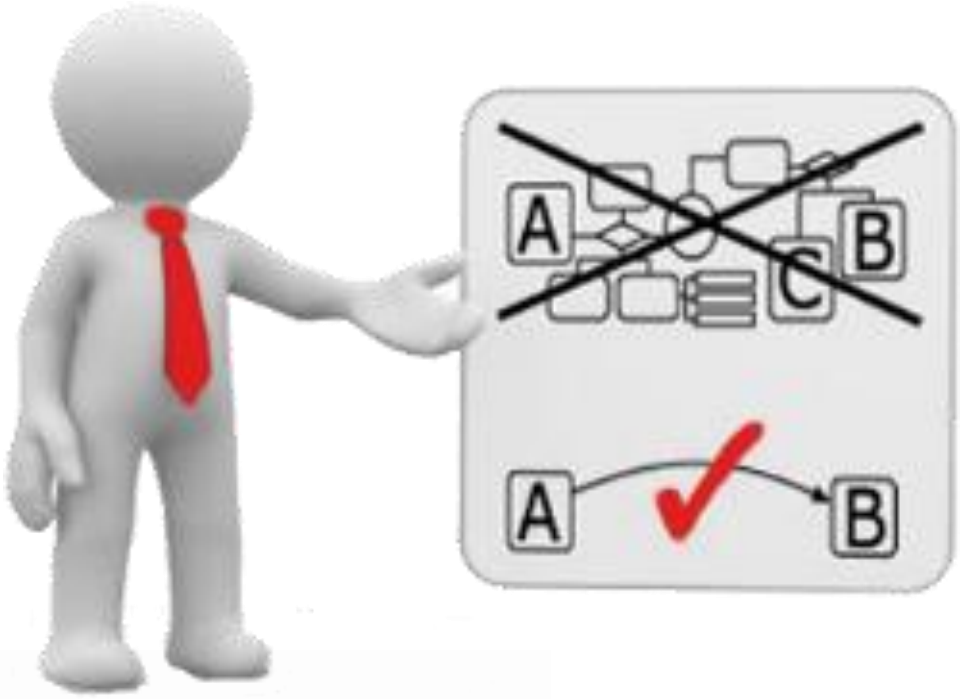
b) Debe estar firmado por su representante legal o gerente general.

Plan de acción

Plan de Acción											
Información del Riesgo / Hallazgo		Información del Plan de Acción						Ejecución			
Identificador del Riesgo / Hallazgo	Riesgo o hallazgo que atiende	Identificador de la acción	Acción / actividad	Detalle de la acción / actividad	Prioridad	Área	Responsable	Inicio	Fin	% de avance	Observaciones

Revisiones del plan de acción

a) Los supervisores pueden hacer observaciones al plan de acción, sugerir mejoras o advertir sobre riesgos significativos.



Prórrogas

Solicitud de prórroga

a) Remisión de los productos entregables de la auditoría externa de TI.

b) Para el plan de acción.

Plan de Acción											
Información del Riesgo / Hallazgo		Información del Plan de Acción						Ejecución			
Identificador del Riesgo / Hallazgo	Riesgo o hallazgo que atiende	Identificador de la acción	Acción / actividad	Detalle de la acción / actividad	Prioridad	Área	Responsable	Inicio	Fin	% de avance	Observaciones

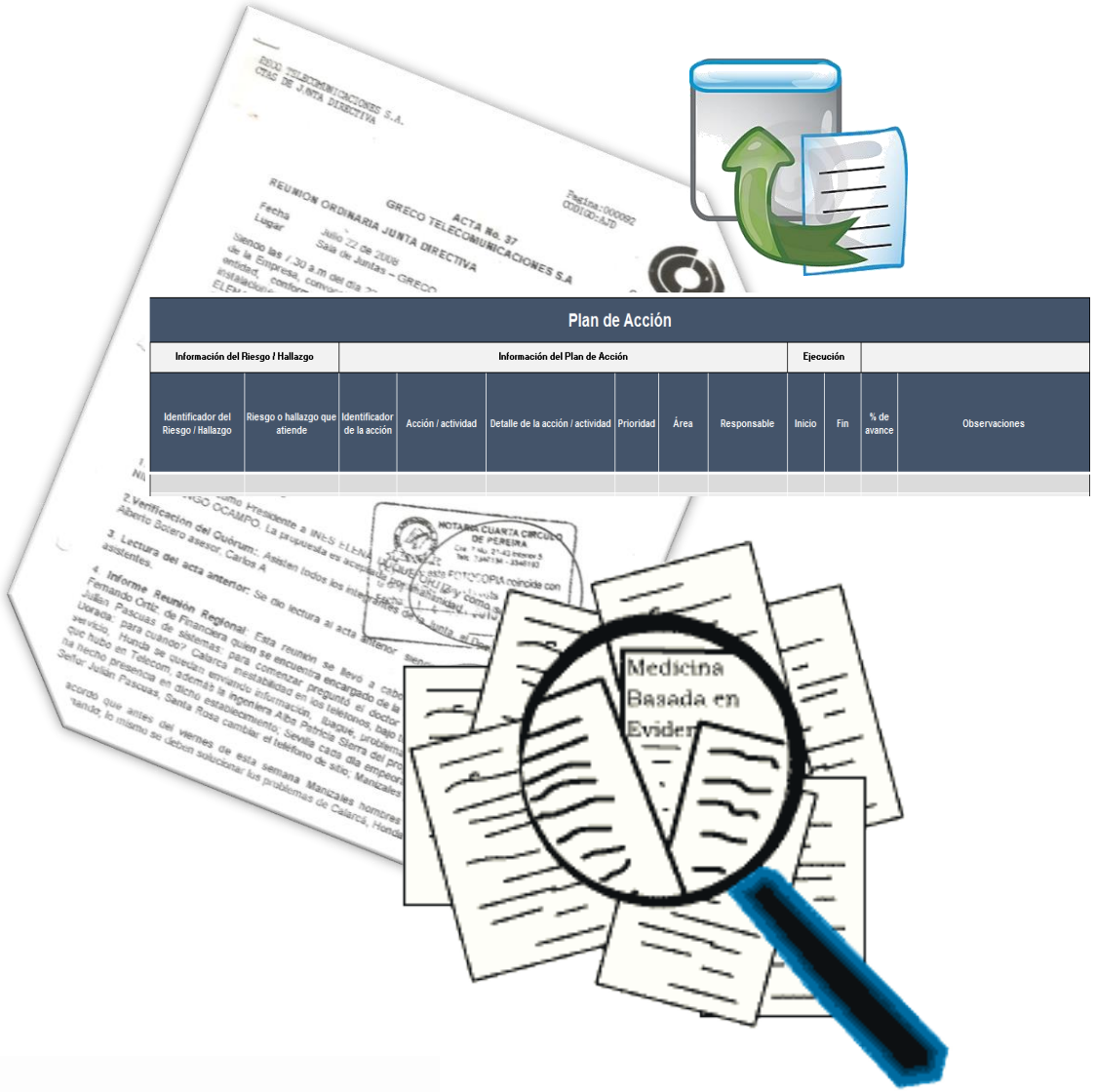
Prórrogas

Responsable

- El representante legal o gerente general de la entidad.

Conteniendo

- Plan de acción, fechas, aprobación correspondiente.
- Motivos y pruebas que imposibilitan a la entidad para cumplir con el plazo original y que fundamenten la solicitud.



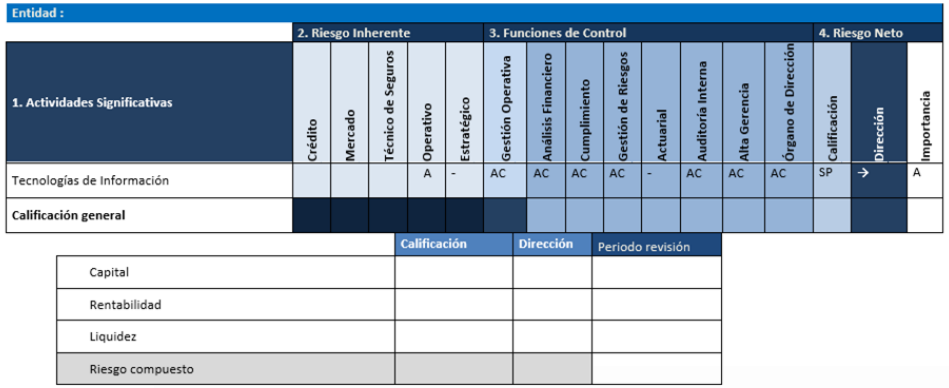
Calificación

Responsabilidad

a) El superintendente, debe emitir la calificación sobre el riesgo de TI de la entidad supervisada.

Metodología

a) La metodología para determinar dicha calificación se establece en las regulaciones particulares de cada Superintendencia.



Entidad :	2. Riesgo Inherente					3. Funciones de Control								4. Riesgo Neto		
1. Actividades Significativas	Crédito	Mercado	Técnico de Seguros	Operativo	Estratégico	Gestión Operativa	Análisis Financiero	Cumplimiento	Gestión de Riesgos	Actuarial	Auditoría Interna	Alta Gerencia	Órgano de Dirección	Calificación	Dirección	Importancia
Tecnologías de Información				A	-	AC	AC	AC	AC	-	AC	AC	AC	SP	→	A
Calificación general																

	Calificación	Dirección	Periodo revisión
Capital			
Rentabilidad			
Liquidez			
Riesgo compuesto			

SUGEF SUPEN SUGESE SUGEVAL

Bases de datos

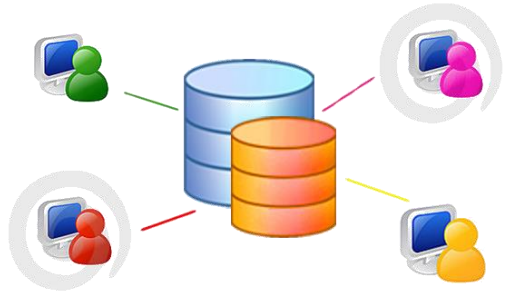
i) Base de datos

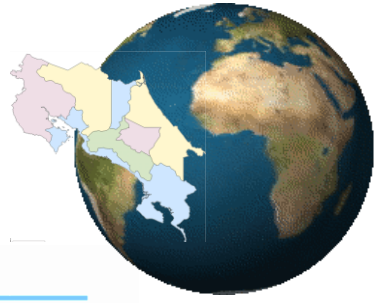
SUGEF SUPEN SUGESE SUGEVAL

Bases de datos

Acceso

El ente supervisor tendrá acceso, sin ningún tipo de restricción o condición, a las bases de datos actualizadas, así como a las aplicaciones vigentes que procesan o dan acceso a estas bases.





Bases de datos

Computación en la nube

Requisitos

- Cumplir con el marco legal, de seguridad y de acceso a la información.

Restricciones del uso de computación en la nube

- Incumplimiento de requisitos legales y de seguridad.
- No se brinde acceso suficiente al supervisor.
- La información sea sensible o crítica para la continuidad del negocio.
- La computación en la nube represente un riesgo para el sistema financiero
- Cuando afecte los intereses de los clientes.

Plazos y remisión

J) Plazo y remisión

Plazos y remisión

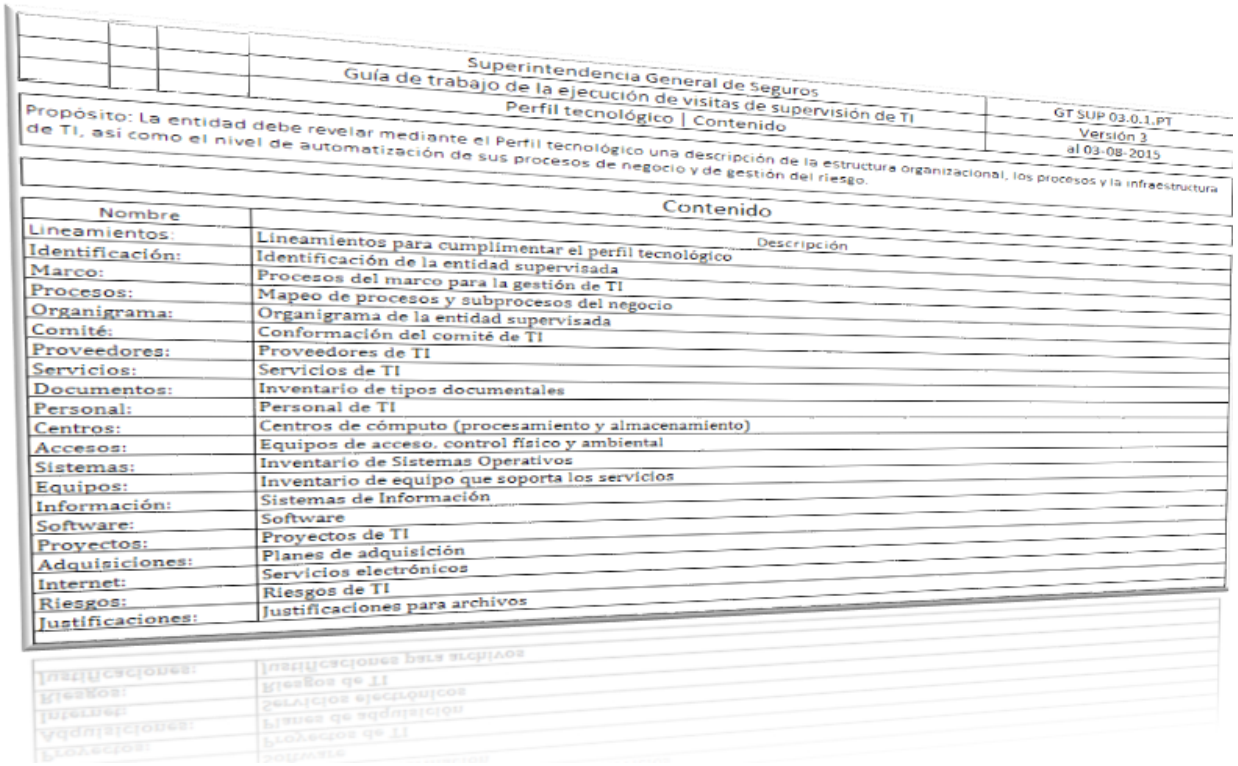
Tipo de gestión de TI

- La solicitud será resuelta en un plazo de 20 días hábiles a partir de la recepción de dicha solicitud y su documentación.
- La Superintendencia podrá requerir información complementaria, dicho requerimiento suspende el plazo de resolución.

Plazos y remisión

Perfil tecnológico

- Remitido anualmente.
- El formato del archivo y su medio de remisión, serán comunicados por medio de circular.
- En caso de ser un conglomerado financiero, se remitirá un único perfil tecnológico.



Superintendencia General de Seguros
Guía de trabajo de la ejecución de visitas de supervisión de TI
Perfil tecnológico | Contenido

GT SUP 03.0.1.PT
Versión 3
al 03-08-2015

Propósito: La entidad debe revelar mediante el Perfil tecnológico una descripción de la estructura organizacional, los procesos y la infraestructura de TI, así como el nivel de automatización de sus procesos de negocio y de gestión del riesgo.

Nombre	Contenido
	Descripción
Lineamientos:	Lineamientos para cumplimentar el perfil tecnológico
Identificación:	Identificación de la entidad supervisada
Marco:	Procesos del marco para la gestión de TI
Procesos:	Mapeo de procesos y subprocesos del negocio
Organigrama:	Organigrama de la entidad supervisada
Comité:	Conformación del comité de TI
Proveedores:	Proveedores de TI
Servicios:	Servicios de TI
Documentos:	Inventario de tipos documentales
Personal:	Personal de TI
Centros:	Centros de cómputo (procesamiento y almacenamiento)
Accesos:	Equipos de acceso, control físico y ambiental
Sistemas:	Inventario de Sistemas Operativos
Equipos:	Inventario de equipo que soporta los servicios
Información:	Sistemas de Información
Software:	Software
Proyectos:	Proyectos de TI
Adquisiciones:	Planes de adquisición
Internet:	Servicios electrónicos
Riesgos:	Riesgos de TI
Justificaciones:	Justificaciones para archivos

Plazos y remisión

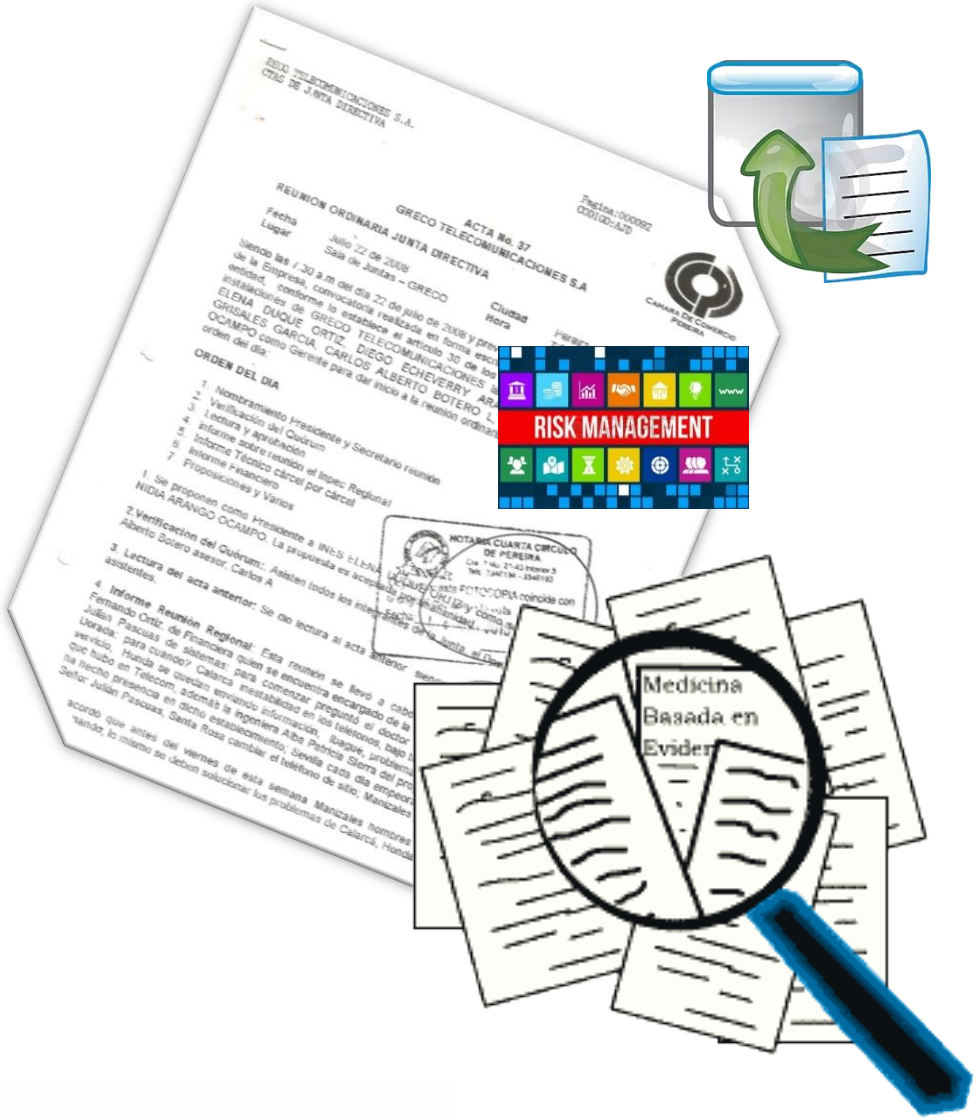
Alcance y plazo de la auditoría

- Productos entregables no debe ser mayor a nueve meses.
- Adicionalmente, las Superintendencias pueden requerir en un plazo menor esos productos de acuerdo a la definición de riesgo que represente la Entidad para la Supervisión.

Plazos y remisión

Alcance y plazo de la auditoría

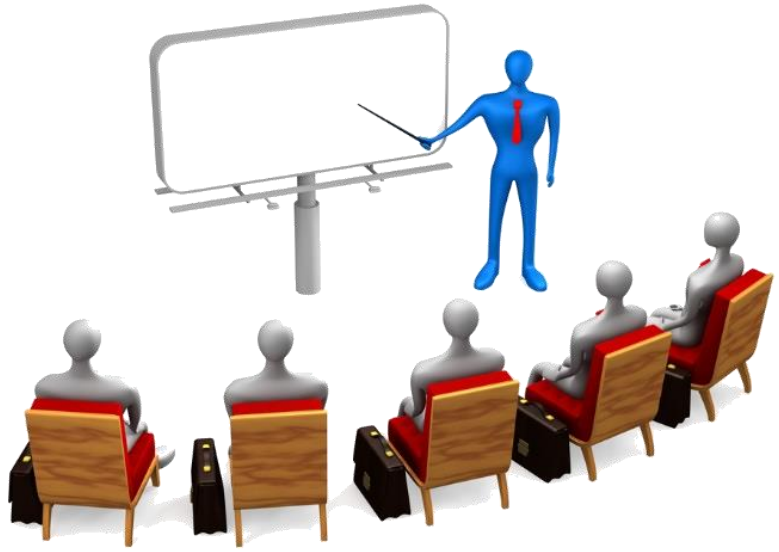
- La entidad supervisada puede presentar una **solicitud de prórroga** ante el supervisor.
- A más tardar ***veinte días hábiles*** **antes del vencimiento del plazo para la remisión de los productos** entregables de la auditoría externa de TI,
- A fin de que la misma pueda ser conocida y resuelta por la respetiva superintendencia.



Plazos y remisión

Presentación de resultados de la auditoría externa

- Las entidades supervisadas deben convocar, previa coordinación con el supervisor, una reunión de salida para la presentación de los resultados de la auditoría externa de TI.
- En el plazo **de cinco días hábiles contados a partir del recibo de los productos de la auditoría** por parte del supervisor.



Plazos y remisión

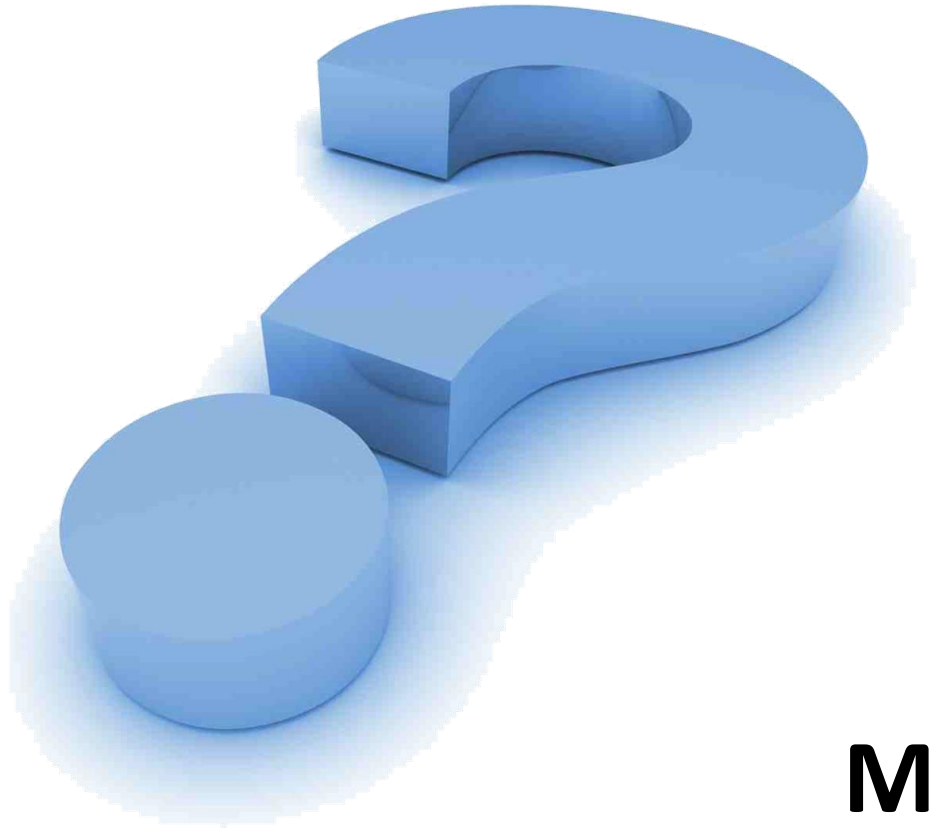
Reporte de supervisión

- Las **superintendencias** deben remitir a la **entidad** el reporte de supervisión,
- En un plazo de veinte días hábiles contados a partir de la reunión de salida para presentar los resultados de la auditoría externa,
- Cuando los supervisores soliciten cambios al informe de auditoría externa, el plazo inicia con la entrega definitiva del informe.

Plazos y remisión

Plan de acción

- La **entidad** puede presentar una **solicitud de prórroga** ante el supervisor.
- De conformidad con los plazos que para el efecto dispone la Ley General de Administración Pública, a fin de que la misma pueda ser conocida y resuelta por la respetiva superintendencia.
- Debe incluir la frecuencia de presentación de informes de avance con plazos no mayores a 6 meses.



Muchas Gracias!!!

SUGEF SUPEN SUGESE SUGEVAL